


National Communications System



Ensuring Essential Communications for the Homeland

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 2002		2. REPORT TYPE		3. DATES COVERED 00-00-2002 to 00-00-2002	
4. TITLE AND SUBTITLE National Communications System: Ensuring Essential Communications for the Homeland				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) National Communications System (NCS),701 South Courthouse Road,Arlington,VA,22204-2198				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 100	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



As the NCS moves into the new Department of Homeland Security, it remains committed to delivering necessary communications for the Federal Government. The NCS has a long history of productive relations both within the Federal Government, and, importantly, within the telecommunications and related industries. The NCS will build on this history of cooperation and will serve as a model for other Government entities as it assumes its new homeland security responsibilities.



NATIONAL COMMUNICATIONS SYSTEM

Ensuring Essential
Communications for the
Homeland

Prepared by the Office of the Manager,
National Communications System

FOREWORD

For nearly 40 years, the men and women of the National Communications System (NCS) have served the country as leaders in national security and emergency preparedness (NS/EP) communications. During these four decades, some of the best and brightest telecommunications engineers, program managers, and staff have dedicated their time and effort to the NCS, working with our industry partners to design, create, and enhance the way we provide emergency communications to Government leadership, first responders, and those who manage our critical infrastructures.

The events of September 11, 2001, forever changed the focus of emergency telecommunications response. Thanks to our National Coordinating Center for Telecommunications (NCC) and established NCS programs, such as the Government Emergency Telecommunications Service (GETS) and the Telecommunications Service Priority (TSP) program, we responded quickly to coordinate and restore emergency communications to areas devastated by the attacks. In our emergency response, we greatly improved important dialogue and cooperation with the Nation's critical infrastructure leaders, and we established new bonds with State and local Government leaders and emergency responders. These actions created a tremendous NS/EP communications team with the common goal of quickly restoring telecommunications services to a country shocked by global terrorism.

The effort to better protect our Nation and its citizens prompted the President to establish an Office of Homeland Security in October 2001 and later to foster the creation of the Department of Homeland Security—the largest reorganization of the Federal Government since

1947. The new Department—with over 170,000 people from 22 Federal organizations—was established on January 24, 2003, with the mission of defending America's homeland. I am proud to say that the NCS is one of the organizations that will expand its role in critical infrastructure protection and homeland security by joining the new Department.

Slated to become part of the new Department's Information Analysis and Infrastructure Protection Directorate, the NCS moves with a longstanding, 40-year history and a multitude of successes in NS/EP communications. The NCS programs and services have grown tremendously since the September 11 attacks. Government leaders, emergency responders, and private companies responsible for the Nation's critical infrastructures have stepped up their contingency efforts to ensure they will be able to respond to meet the country's emergency needs.

In addition to our successful programs, the NCS is bringing new technologies to the Department. Congestion in certain areas for wireless communications during the September 11 attacks accelerated the creation of Wireless Priority Service (WPS). Last May, the NCS established an interim WPS in New York and Washington. In late 2002, the NCS will start deploying WPS nationwide, with the goal of providing full coverage by the end of 2003.

Other new programs in development—such as the Global Early Warning Information System (GEWIS), the Cyber Warning Information Network (CWIN), the Emergency Notification System (ENS), and Back-up Dial Tone (BDT)—will provide the Department new ways to communicate emergency messages to senior leaders of Government and industry as well as to the American public.

Finally, our longstanding tradition of partnership with other Government entities and the telecommunications industry is a model that other infrastructures strive to emulate. The Committee for National Security and Emergency Preparedness Communications and its Council of Representatives, the President's National Security Telecommunications Advisory Committee and its Industry Executive Subcommittee, the National Coordinating Center for Telecommunications, the Network Security and Information Exchanges, and the Telecommunications Information Sharing and Analysis Center (plus dozens of other Government/industry relationships) have built a tremendous trusted network of professionals focused on the Nation's emergency communications. These relationships remain a pillar of strength that will greatly benefit the new Department of Homeland Security.

Our team is a group of individuals and organizations sharing mutually beneficial goals toward a unified mission. For 40 years, the NCS goals and mission have been to coordinate emergency communications for the protection of our country and its citizens. It is only fitting that these professional communicators, the programs we continue to build, and the partnerships we've established over the years, move to a new team – a team designed to continue the work we've been doing for four decades. As I prepare to relinquish my duties with the NCS, I am excited about NCS' future and the new challenges this organization will face in the years to come.

A handwritten signature in black ink, appearing to read "Harry D. Raduege, Jr.", written in a cursive style.

Lieutenant General Harry D. Raduege, Jr.
Manager



NCS LEADERSHIP



Lieutenant General Harry D. Raduege, Jr.
Manager



Mr. Brenton C. Greene
Deputy Manager



CAPT J. Katharine Burton
Assistant Deputy Manager



Dr. Peter A. Fonash
*Chief
Technology and
Programs Division*



Mr. Frederick W. Herr
*Chief
Critical Infrastructure
Protection Division*



Mr. Larry E. Wheeler
*Chief
Plans and
Resources Division*



Col. Wilson D. Crafton
*Chief
Customer Service
Division*

NCS COMMITTEE FOR NATIONAL SECURITY AND EMERGENCY PREPAREDNESS COMMUNICATIONS



*Department of State
(DOS)*
MR. FERNANDO BURBANO



*Department of the Treasury
(TREAS)*
MR. THOMAS C. WEISNER



*Department of Defense
(DOD)*
MR. STEVEN PRICE



*Department of Justice
(DOJ)*
MR. MICHAEL D. DUFFY



*Department of the Interior
(DOI)*
MR. DARYL W. WHITE



*Department of Agriculture
(USDA)*
MR. IRA L. HOBBS



*Department of Commerce
(DOC)*
MS. KAREN F. HOGAN



*Department of Health and
Human Services (HHS)*
DR. ROBERT KNOUSS



*Department of
Transportation (DOT)*
MR. EUGENE K. TAYLOR, JR.



*Department of Energy
(DOE)*
MS. KAREN EVANS



*Department of Veterans
Affairs (VA)*
MR. EDWARD F. MEAGHER



*Federal Emergency
Management Agency
(FEMA)*
MR. JOSEPH D. SZWARCOP



The Joint Staff (JS)
LTG JOSEPH K. KELLOGG, JR.
USA



*General Services
Administration (GSA)*
MS. SANDRA N. BATES



*National Aeronautics and
Space Administration
(NASA)*
MR. ROBERT E. SPEARING



*Nuclear Regulatory
Commission (NRC)*
MR. RICHARD WESSMAN



*National Telecommunications
and Information
Administration (NTIA)*
MR. FREDERICK R. WENTLAND



*National Security Agency
(NSA)*
MR. MICHAEL G. FLEMING



*United States Postal Service
(USPS)*
MR. TIMOTHY J. PATTERSON



*Federal Reserve Board
(FRB)*
MR. KENNETH D. BUCKLEY



*Federal Communications
Commission (FCC)*
MR. JEFFREY M. GOLDTHROP

NCS Council of Representatives

F I S C A L Y E A R 2 0 0 2



*Department of State
(DOS)*
MS. KIMBERLY A. GODWIN



*Department of the Treasury
(TREAS)*
MR. EDD BARNES



*Department of Defense
(DOD)*
CAPT LYNNE HICKS, USN



*Department of Justice
(DOJ)*
MR. GARY W. LAWS



*Department of the Interior
(DOI)*
MR. JAMES E. DOLEZAL



*Department of Agriculture
(USDA)*
MS. BRENDA F. BOGER



*Department of Commerce
(DOC)*
MR. BENJAMIN CHISOLM



*Department of Health and
Human Services (DHHS)*
CAPT MICHAEL B.
ANDERSON, USPHS



*Department of
Transportation (DOT)*
MR. JAMES HARRELL



*Department of Energy
(DOE)*
MR. GORDON ERRINGTON



*Department of Veterans
Affairs (VA)*
MR. DAVID CHEPLICK



*Federal Emergency
Management Agency
(FEMA)*
MR. PAUL B. MAISON



The Joint Staff (JS)
COL JOHN REIDT



*General Services
Administration (GSA)*
MR. THOMAS E. SELLERS



*National Aeronautics and
Space Administration (NASA)*
MR. JOHN C. RODGERS



*Nuclear Regulatory
Commission (NRC)*
MR. NADER L. MAMISH



*National Telecommunications
and Information
Administration (NTIA)*
MR. WILLIAM A. BELOTE



*National Security Agency
(NSA)*
MR. GILBERT C. NOLTE



*United States Postal
Service (USPS)*
MR. TIMOTHY J. PATTERSON

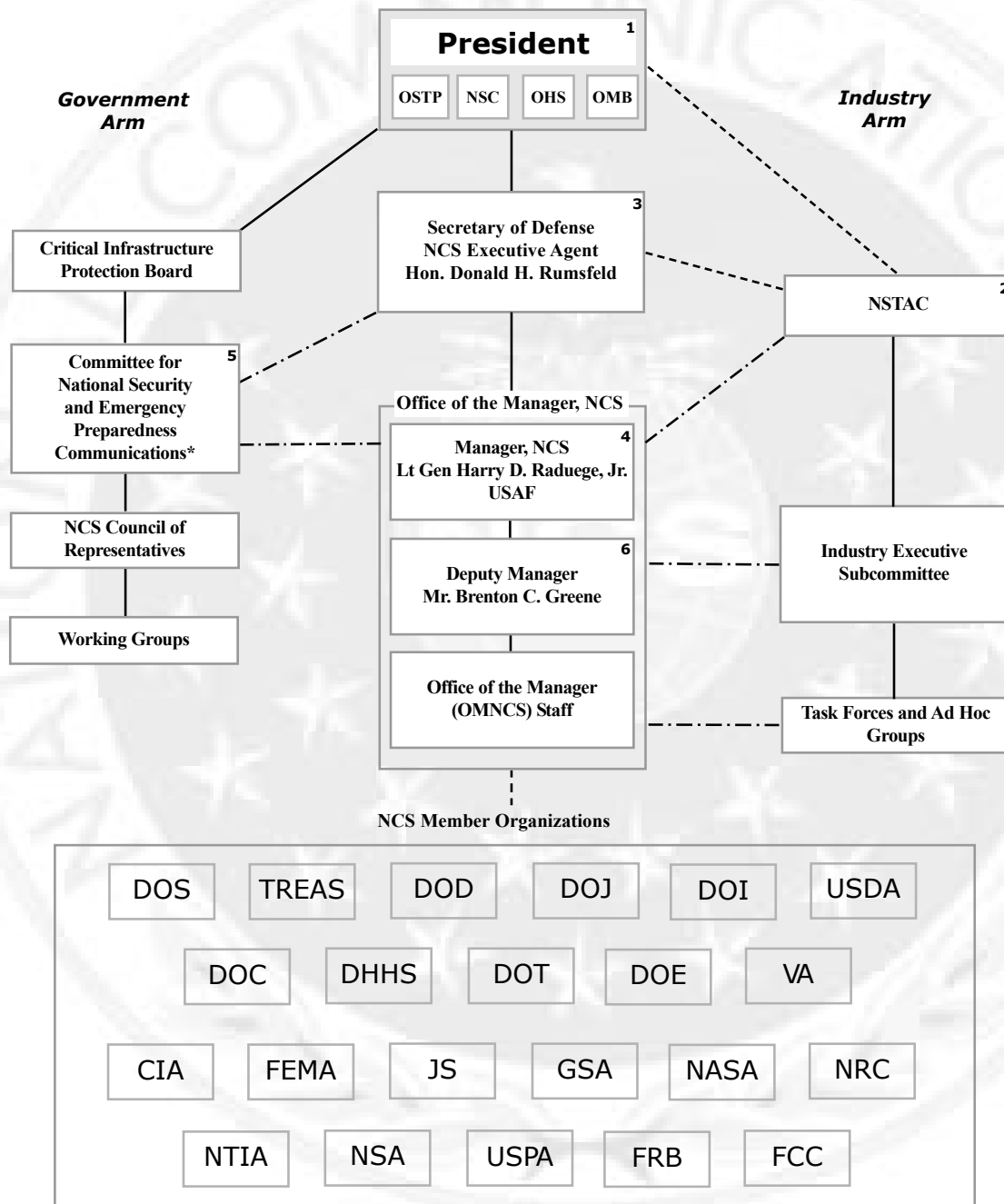


*Federal Reserve Board
(FRB)*
DR. H. WAYNE PACINE



*Federal Communications
Commission (FCC)*
MR. KENNETH P. MORAN

THE NCS STRUCTURE



1. Policy Direction and Direct Execution of War Powers Function
2. National Security Telecommunications Advisory Committee created by E.O. 12382
3. Executive Agent, NCS responsibilities assigned to Secretary of Defense by E.O. 12472, April 3, 1984
4. Director, DISA, serves as Manager, NCS
5. The Key Telecommunications Officers of the NCS Member Organizations who form one of 11 standing committees under the President's Critical Infrastructure Protection Board, created by E.O. 13231, October 16, 2001
6. First line management position that is exclusively NCS

TABLE OF CONTENTS

	<i>Page Number</i>		<i>Page Number</i>
I. INTRODUCTION/HISTORY OF THE NATIONAL COMMUNICATIONS SYSTEM	2-I	Department of Justice (DOJ)	8-V
<hr/>		Department of Interior (DOI)	9-V
II. ENVIRONMENT FACING THE NATIONAL COMMUNICATIONS SYSTEM		U.S. Department of Agriculture (USDA)	10-V
Recovering from September 11, 2001	2-II	Department of Commerce (DOC)	11-V
Wireless Communications	3-II	Department of Health and Human Services (DHHS)	12-V
Network Security	4-II	Department of Transportation (DOT)	13-V
Network Convergence	5-II	Department of Energy (DOE)	15-V
Report Organization	6-II	Department of Veterans Affairs (VA)	16-V
<hr/>		Central Intelligence Agency (CIA)	17-V
III. EMERGENCY RESPONSE ACTIVITIES		Federal Emergency Management (FEMA)	18-V
September 11, 2001, Response Assessment	2-III	The Joint Staff (JS)	19-V
WPS at the Winter Olympics	3-III	General Services Administration (GSA)	20-V
<hr/>		National Aeronautics and Space Administration (NASA)	24-V
IV. NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS		Nuclear Regulatory Commission (NRC)	25-V
Technology and Programs Division	3-IV	National Telecommunications and Information Administration (NTIA)	26-V
Critical Infrastructure Protection Division	12-IV	National Security Agency (NSA)	28-V
Plans and Resources Division	24-IV	U.S. Postal Service (USPS)	30-V
Customer Service Division	25-IV	Federal Reserve Board (FRB)	32-V
<hr/>		Federal Communications Commission (FCC)	33-V
V. NS/EP TELECOMMUNICATIONS SUPPORT AND ACTIVITIES OF NCS MEMBER ORGANIZATIONS		<hr/>	
Department of State (DOS)	2-V	A. NCS RELATED ACRONYMS	
Department of Treasury (TREAS)	4-V		
Department of Defense (DOD)	6-V		





I

INTRODUCTION

THE HISTORY OF THE NATIONAL COMMUNICATIONS SYSTEM

18	IDED8
17	IDED9
16	IDED10
15	IDED11
14	IDED12
13	IDED13
12	IDED14
11	IDED15

INTRODUCTION

THE HISTORY OF THE NATIONAL COMMUNICATIONS SYSTEM

This document, prepared by the Office of the Manager, National Communications System (NCS), reports on national security and emergency preparedness (NS/EP) activities and telecommunications events, and highlights the agency's innovations, programs, and achievements during fiscal year 2002.

President John F. Kennedy established the NCS in 1963 as a result of the communications issues discovered during the 1962 Cuban missile crisis. During critical periods of the crisis, there was tremendous difficulty in establishing and maintaining communications between the U.S., the Union of Soviet Socialist Republics, the North Atlantic Treaty Organization, and foreign heads of state, which proved detrimental to the resolution efforts. Following the crisis, President Kennedy mandated the National Security Council (NSC) to conduct an investigation regarding national security communications. In response, the NSC established an interdepartmental committee to evaluate critical communications networks and make changes as needed to meet the Nation's requirements.

To best serve the needs of the President, the Department of Defense, diplomatic and intelligence agencies, and civilian leadership, the NSC committee found that a consolidated system would be required. This system would



support critical Government communications functions, especially during periods of heightened national security or in times of crisis; hence, the creation of the NCS. Established by Presidential Memorandum on August 21, 1963, the NCS is responsible for ensuring NS/EP communications function successfully, including interconnectivity and survivability during times of congestion or when the networks have been damaged or destroyed. When brought to light, NS/EP communications remained in the forefront of Presidential concern in the Nation's defense. On April 3, 1984, President Ronald Reagan signed Executive Order (E.O.) 12472, which superceded President Kennedy's Memorandum on the NCS. This E.O. assigned the NCS with the mission to assist the President; the NSC; the Director; Office of Science and Technology Policy; and

the Director, Office of Management and Budget in coordinating the planning for and provision of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery and reconstitution, and ensuring the national telecommunications infrastructure is developed. Nearly 40 years after the NCS was created, this remains the core responsibility of the NCS.

As a result of the September 11, 2001, terrorist attacks on the World Trade Center in New York and the Pentagon in Washington, DC, President George W. Bush issued E.O. 13228 (October 8, 2001) and E.O. 13231 (October 16, 2001). These orders further defined the role of the NCS in national and homeland security.

E.O. 13228 established the White House Office of Homeland Security (OHS) and tasked the OHS to coordinate efforts to protect critical public and privately owned information systems within the U.S. from terrorist attacks. The OHS was also mandated to coordinate the efforts that would ensure the rapid restoration of telecommunications and critical information systems after disruption by a terrorist threat or attack.

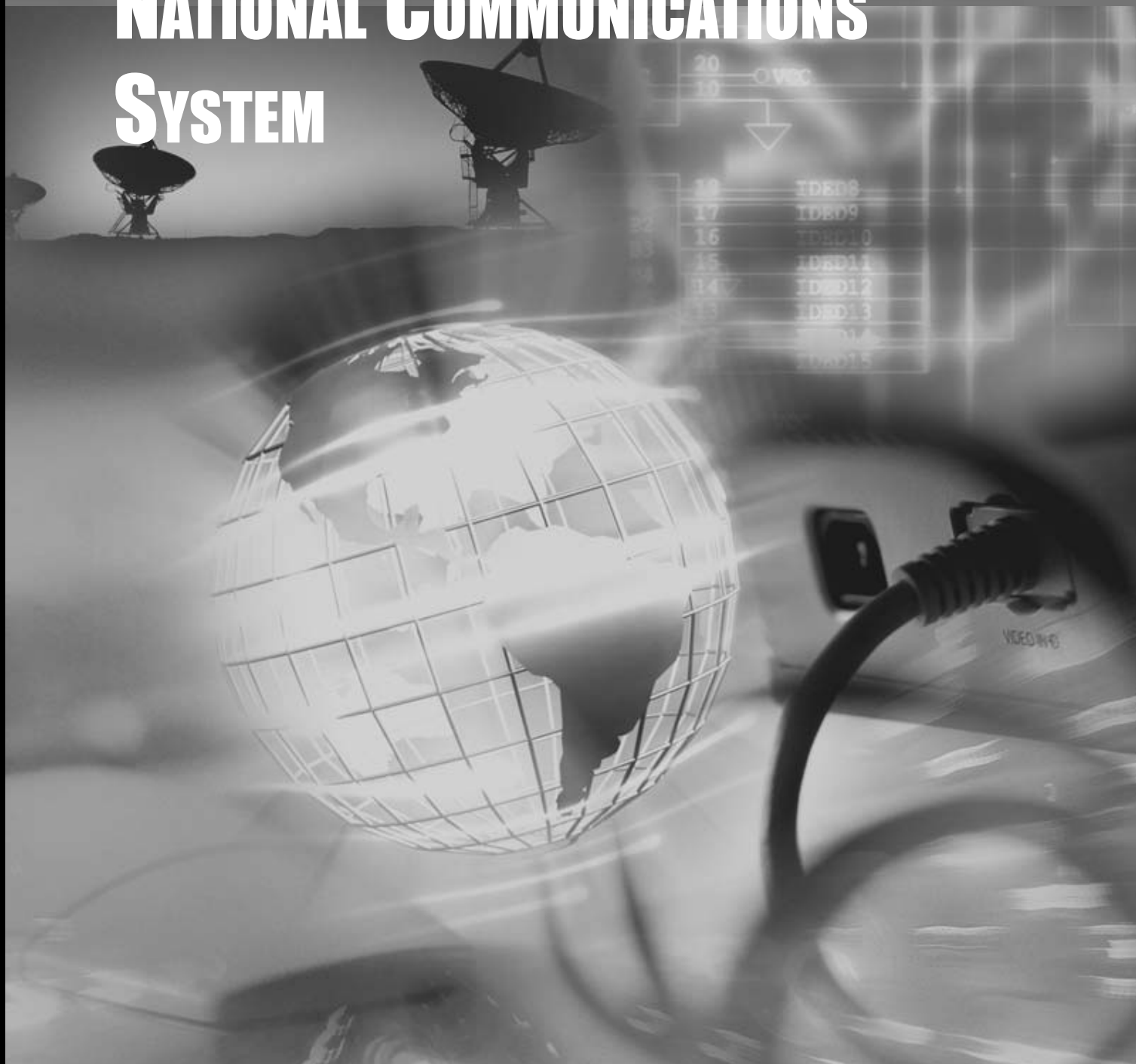
The establishment of the President's Critical Infrastructure Protection (CIP) Board with E.O. 13231 renamed the NCS Committee of Principals as the Committee for National Security and Emergency Preparedness Communications (NS/EPC) and assigned the group as a permanent standing committee of the OHS. E.O. 13231 reiterated the reporting functions and responsibilities established in E.O. 12472 for the NCS and for the NS/EPC. The Chair of the CIP Board (currently the President's Special Advisor for Cyberspace Security), in addition to his responsibilities with nearly a dozen CIP Board committees, also works closely with panels of senior experts from outside the Government. This includes the President's National Security Telecommunications Advisory Committee, created by E.O. 12382 in September of 1982.

All of these E.O.s reinforce the important role the NCS plays in national security and homeland defense. The NCS has evolved throughout its history to meet the demands of a changing environment and continues to provide proactive solutions to current and future requirements.



II

ENVIRONMENT FACING THE NATIONAL COMMUNICATIONS SYSTEM



ENVIRONMENT FACING THE NATIONAL COMMUNICATIONS SYSTEM

RECOVERING FROM SEPTEMBER 11, 2001

The events of September 11, 2001, required the National Communications System (NCS) and industry to marshal resources at the National, State, and local levels to support response and recovery efforts. The restoration and provisioning of emergency communications services to emergency personnel was a critical part of those efforts. The NCS and its National Coordinating Center for Telecommunications (NCC), in partnership with private companies, played a major role in ensuring a quick response and recovery of telecommunications capabilities in the wake of the September 11 attacks.

The Federal Government has since been revisiting how it will deal with future threats to homeland security. In October 2001, President Bush created the Office of Homeland Security (OHS), headed by Governor Tom Ridge, within the Executive Office of the President to serve as a focal point for homeland security issues. After careful study of the Federal Government's current structure, OHS found responsibilities for homeland security dispersed among more than 100 different agencies, and therefore, identified a significant need to create a single agency with a homeland security mission.

Consequently, in June 2002, the President proposed the creation of the Department of Homeland Security (DHS), a Cabinet-level agency with a clear mission: to serve as a "single, unified homeland security structure that will improve protection against today's threats and be flexible enough to help meet the unknown threats of the future." The Administration recommended that the NCS be part of the proposed DHS along with the homeland security assets of the Departments of the Treasury, Justice, Commerce, Transportation, Energy, Health and Human Services, and the Federal Emergency Management Agency. DHS would serve as the single point for coordination and communication with state and local governments, the private sector, and the public, and would develop a major intelligence analysis capability to support homeland security operations.

In July 2002, the White House released the President's National Strategy for Homeland Security, which provides a framework to further guide Federal, State and local, and private sector homeland security efforts. The National Strategy seeks to provide initial direction to the Government and private sector, and establish priorities for the work ahead. The National Strategy builds upon three strategic objectives of homeland security:

SEVERE SEVERE RISK OF TERRORIST ATTACK
HIGH HIGH RISK OF TERRORIST ATTACK
ELEVATED SIGNIFICANT RISK OF TERRORIST ATTACK
GUARDED GENERAL RISK OF TERRORIST ATTACK
LOW LOW RISK OF TERRORIST ATTACK

- Prevent terrorist attacks within the U.S.
- Reduce America's vulnerability to terrorism and
- Minimize the damage and recover from attacks that do occur.

Building upon the Administration's proposal for the creation of the DHS, the National Strategy outlines six critical mission areas:

- Intelligence and warning
- Border and transportation security
- Domestic counter terrorism
- Protecting critical infrastructure
- Defending against catastrophic terrorism and
- Emergency preparedness and response.

Currently, the NCS supports and operates many national security and emergency preparedness (NS/EP) programs that would provide a valuable foundation for the DHS, particularly within the areas of critical infrastructure and emergency preparedness and response.

WIRELESS COMMUNICATIONS

The attacks of September 11, 2001, bring to the forefront the need for secure and reliable emergency wireless service. Wireless technologies are increasingly being used for voice, data, and video transmissions, including communications in support of national security and emergency preparedness (NS/EP) missions. The NCS is working to better understand security requirements and identify potential wireless vulnerabilities. In conjunction with the President's National Security Telecommunications Advisory Committee (NSTAC), the NCS is undertaking activities to determine where wireless vulnerabilities exist,

including customer devices, network interfaces, and facilities. With a clearer understanding of these vulnerabilities, the NCS is better positioned to effectively coordinate plans and policies to protect wireless communications.

A specific focus of NCS wireless activity is the establishment and development of the Wireless Priority Service (WPS). The NCS is administering the WPS program to enable NS/EP leaders and key personnel to have priority access and treatment during crisis events and emergency scenarios during which high call volumes could cause severe wireless network congestion. The NCS has been involved in WPS research, planning, and rulemaking for several years, and in FY 2002, led the implementation of WPS capabilities.

In the post September 11 environment, the NCS and the Administration began implementing the WPS program in two phases. The interim phase was dedicated to deploying an immediate WPS



The 2002 Winter Olympics in Salt Lake City, Utah, was used as a pilot test of WPS.

solution for Washington, D.C. and New York City, New York, following a successful test of wireless priority capabilities during the 2002 Winter Olympic Games in Salt Lake City, Utah. The second phase involved working with the wireless industry to develop and deploy an initial nationwide WPS solution. The NCS is also involved in the design and implementation of the WPS full operating capability (FOC), scheduled for completion in late 2003.

The WPS FOC is expected to be an end-to-end service, fully integrated with the Government Emergency Telecommunications Service (GETS) program, which addresses congestion on wireline networks.

The NCS is also working to ensure that the WPS user base, including State and local governments and NS/EP entities, is becoming more aware of the service and its benefits. Through coordination with these bodies, the NCS will be better able to determine how the service could be deployed.

Network Security

CYBERSPACE STRATEGY

FY 2002 saw a continued rise in the number of cyber-related incidents threatening U.S. information and communications networks. Representatives of Carnegie Mellon's Computer Emergency Response Team Coordination Center (CERT/CC), indicated that they received reports of 73,359 cyber incidents and 3,222 vulnerabilities in the first three quarters of 2002 alone, representing a significant increase over the totals reported for all of 2001. A major security concern during the year was the discovery of vulnerabilities in the simple network management protocol (SNMP). Both Government and industry spent considerable time and money identifying SNMP vulnerabilities in their systems and repairing them. While many of the network attack techniques used in FY 2002 were familiar, new trends in technology and attack methods emerged such as:

- Worms with faster methods of self-propagation, resulting in an increased number of compromised U.S. computers ("zombies") with high bandwidth connections
- An increased number and frequency of automated attacks, including widespread distributed denial of service (DDoS) attacks
- An increase in sophistication of attacks, especially "blended" attacks, i.e., exploits composed of a combination of worms, viruses, and/or Trojans
- A decrease in the time needed by adversaries to discover vulnerabilities along with quicker and broader methods for adversaries to exploit vulnerabilities and
- An increased ability to bypass firewalls using technologies such as the Internet Printing Protocol (IPP) and Internet Relay Chat (IRC).

In response to both September 11 and the growing threats to cyberspace, the President's Critical Infrastructure Protection Board published its draft National Strategy to Secure Cyberspace in September 2002 to help mitigate the effects of future Internet attacks. The Cyberspace strategy provides a framework to secure the information technology networks and systems that support the Nation's critical infrastructures and is in line with the Administration's previously released the Strategy for Homeland Security. The Cyberspace strategy discusses how both corporate and home users can protect their networks, and provides further guidance to Federal, state, and local governments. The draft will be updated periodically as the network security environment evolves.

VULNERABILITY OF

TELECOMMUNICATIONS ASSETS

Over the past year, the NCS supported various efforts to ensure the protection and viability of the telecommunications infrastructure. In February 2002, the Special Advisor to the President for Cyberspace Security requested the NCS conduct an analysis of the vulnerabilities of the intercontinental submarine cable system. Given the concern that the destruction or damage to this system could severely impact the U.S. economic and national security posture, the NCS was tasked to:

- Identify the submarine fiber optic cables with landing points here in the U.S.
- Determine the degree to which these cables are concentrated in a few switching centers
- Investigate current security measures to protect those assets and
- Conduct an impact analysis to determine what would happen if one or more of these switching centers or landing points were damaged.

In addition to responding to these requests, the NCS recommended additional areas of analysis to further evaluate additional redundancy and diversity for the submarine cable system and address other security measures.

In March 2002, the Special Advisor for Cyberspace Security asked the NCS to examine risks stemming from the concentration of telecommunications assets and fiber optic cable at certain locations throughout the U.S. The focus was to identify these points of concentration and conduct a preliminary impact analysis. The NCS is also working with the Network Reliability and Interoperability Council (NRIC) to assess the physical vulnerabilities in the public telecommunications networks, including the Internet, and to define best practices for preventing significant disruptions.

NETWORK CONVERGENCE

Telecommunications carriers are implementing cost-effective networks to remain competitive in the evolving telecommunications marketplace and to support wide-scale delivery of diverse, advanced broadband services. However, because of their large investments in public switched telephone network (PSTN) infrastructure, carriers are initially leveraging the best of both infrastructures, resulting in a period of network convergence during the transition to the next generation network (NGN). In this evolving network environment, the NCS recognizes

industry and Government must strive to identify and remedy associated network vulnerabilities to ensure sustained critical communications capabilities of the NS/EP community.

The NCS is actively participating in various domestic and international standards bodies to establish a comprehensive family of standards for an Emergency Telecommunications Service (ETS) in next generation networks and to ensure that NS/EP functional requirements are considered during convergence to the NGN. The ETS standards initiative is currently being developed in partnership with the telecommunications industry in major national and international standards bodies such as the European Telecommunications Standards Institute's (ETSI) Telecommunications and Internet Protocol Harmonization over Networks (TIPHON) working groups. These efforts address the issues of adding mechanisms to the new protocols and signaling systems to support priority services for preferential handling of ETS communications. This is a multidimensional effort addressing myriad issues that will ensure the provisioning of a comprehensive and effective ETS in future networks.

The NCS is also actively participating in the International Telecommunications Union's Standardization Sector (ITU-T) efforts regarding the International Emergency Preference Scheme (IEPS). IEPS recognizes the requirement for priority communications among Government, civil, and other essential users of public telecommunications services in crisis situations. IEPS, which is similar to GETS, would give authorized users priority access to and transport of NS/EP-related calls on an international basis within the PSTN infrastructure and specifically with the Integrated Services Digital Network (ISDN) infrastructures.

Over the past year, in conjunction with the White House Office of Science and Technology Policy (OSTP), the NCS also took part in the Interagency Convergence Subgroup activities. The group addressed issues associated with the convergence of the voice and data networks and

the implications of this convergence on NS/EP telecommunications services. The task force identified several recommendations on how to begin implementing NS/EP services in the converged environment, including the need to establish a baseline for requirements, contract support for security and technical issues, and assign issues to lead agencies. The final report of the Interagency Convergence Subgroup was issued in February 2002.

REPORT ORGANIZATION

The subsequent sections of this report detail the NCS FY 2002 activities and accomplishments undertaken to fulfill the NCS mission. Section 3 describes the emergency response activities of the OMNCS. Section 4 contains a description of OMNCS NS/EP telecommunications support, activities, programs, and major interagency initiatives. Finally, Section 5 reviews the NS/EP telecommunications support and activities of the NCS member organizations.

The FY 2002 National Communications System Report reflects the NCS commitment to meeting the full range of NS/EP telecommunications needs for the Nation under all circumstances.

III

EMERGENCY RESPONSE ACTIVITIES



III

EMERGENCY RESPONSE ACTIVITIES

The National Communication System's (NCS) National Coordinating Center for Telecommunications (NCC) ensures that Federal, State, and local responders receive national security and emergency preparedness (NS/EP) communications support during national disasters. The NCS supports emergency response efforts by training key personnel and provisioning communications resources. It is also the primary agency for implementing and coordinating the Federal Response Plan's Emergency Support Function #2 (ESF #2), coordinating NS/EP communications support to Federal, State, and local officials during emergencies and disasters through the NCC, and assisting in the restoration of the communications infrastructure after a major disaster.

Two groups assist the NCS in carrying out these functions. The first is Individual Mobilizations Augmentees (IMAs) who are Army Reserve Signal Corps officers who serve as a rapid response element to travel to disaster sites representing the NCS. The other group is the General Services Administration's Regional Communications Managers who become NCS Regional Managers following a disaster declaration.

NCS Regional Managers responded to the Southwest wildfires that raged across Utah, Colorado, California, New Mexico, Arizona, South Dakota, North Dakota, Montana, Texas,

and Wyoming sporadically from May until September 2002. The Regional Managers remained on site for 21 days and performed multiple duties to coordinate restoration of communications damaged by the wildfires and provisioning of new communications capabilities for the other response elements. In addition to NCS activities in support of NS/EP communications planning and readiness efforts, the NCS also worked in two other key areas: (1) analyzing September 11, 2001, response activities; and (2) implementing Wireless Priority Service (WPS) capabilities at the 2002 Winter Olympics.

SEPTEMBER 11, 2001 RESPONSE ASSESSMENT

The tragic events of September 11, 2001, required an immediate response by the NCS and made extensive use of the NCC's ability to coordinate restoration activities and share information between industry, Federal, State, and local responders. The sheer magnitude of the response efforts, coupled with the numerous emergency services personnel involved in the September 11 communications restoration, exemplified the emerging challenges that will profoundly impact future NCC operations. While the NCC performed extraordinarily well and was integral to the response efforts, the NCS' after-action assessment highlighted several recommendations that are currently being

addressed. The assessment revealed that the NCS must augment its capabilities in the following areas:

- Plans and procedures
- Communications
- Information sharing and management
- Staff, tools, and facilities resources
- Security and clearances and
- Industry coordination.

Throughout FY 2002, several of the recommendations from the September 11, 2001, Response Assessment were addressed. The NCC is in the process of revising its plans and procedures and has trained additional emergency response staff to ensure that operations from multiple locations can be accomplished, while in the process of upgrading all NCC facilities and equipment. The NCC now operates a full time (24 hours, 7 days a week) operations center, and its telecommunications industry coordination and information sharing potential has been enhanced by a greater commitment from participating members as well as an increase in telecommunications companies in both the NCC and Telecom Information Sharing Assessment Center (ISAC). Further, the NCS provides full time staffing for a desk in the Defense Information Systems Agency (DISA) Global Network Operations and Security Center/Joint Task Force-Computer Network Operations (GNOSC/JTF-CNO) to ensure adequate and effective coordination of DISA and NCS activities. Continuing to implement improvements in these areas will further enhance the NCC's ability to support an all-hazard NS/EP telecommunications response.



WIRELESS PRIORITY SERVICE AT THE WINTER OLYMPICS

In February 2002, the NCS implemented an emergency WPS capability in support of NS/EP communications planning and readiness efforts for the 2002 Winter Olympic Games in Salt Lake City, Utah. Working with the Federal Emergency Management Agency (FEMA), the NCS mobilized IMA's and NCS staff to support the mission and the operations concept for emergency communications support during the Games. The WPS solution for the Olympics involved using enhanced satellite services,

increased trunking, redirection of wireless user calls away from congested areas, and supplemental wireless communications capabilities programmed on satellite communications handsets. Although NS/EP personnel did not use WPS for actual emergencies, response personnel were fully equipped to manage communications in the event of a crisis situation.

The Salt Lake City experience was the beginning for a larger deployment of WPS assets to New York and Washington in FY 2002. Once the NCS implements the Initial Operating Capability in FY 2003, Government officials and key NS/EP personnel will be able to use WPS during emergencies when high call volumes could cause severe wireless network congestion.



IV

NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS



The background of the page is a complex collage. At the top, there are stylized, glowing vertical lines. Below these, on the left, are silhouettes of satellite dishes against a dark sky. In the center, a wireframe globe is shown with a bright light source behind it, creating a lens flare effect. To the right of the globe, there is a technical diagram showing a signal path with a downward arrow and a label 'OVec'. Below this, a list of data points is displayed, each with a number and a label. In the bottom right corner, there is a close-up of a cable connector with the text 'VIDEO IN' visible.

19	IDED8
17	IDED9
16	IDED10
15	IDED11
14	IDED12
13	IDED13
12	IDED14
11	IDED15

IV

NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

This section features the accomplishments and activities of the Office of the Manager, National Communications System (OMNCS), the National Communications System (NCS), and the national security and emergency preparedness (NS/EP) community as it faced many challenging issues during fiscal year (FY) 2002.

ISSUES COVERING THE ENTIRE NCS SPECTRUM

The threat to our Nation's critical infrastructure and, more specifically for the NCS, to the Nation's telecommunications facilities, is one of the Nation's greatest national security concerns. In an effort to establish a solid backbone for telecommunications supporting homeland security, this year the NCS focused particularly on the issues surrounding threat and vulnerability assessments of cyber attacks and critical telecommunications facilities. The NCS also continued to develop a wireless priority system and to explore next generation network evolution and the implications for emergency communications. In addition, the NCS continued its support of existing programs to further interoperable communications networks for the emergency responder community. Through a number of programs and activities detailed in this chapter, the NCS worked to establish programs that address and mitigate these national security concerns. The NCS has also focused on the growing need to unite all

aspects of the national infrastructure to ensure cohesion in national security and emergency preparedness telecommunications through its efforts to link the NCS with other vital players.

TRANSITION TO THE DEPARTMENT OF HOMELAND SECURITY

At the forefront of issues that the NCS faced and continues to face is the role it will play within the Department of Homeland Security (DHS). The NCS took a proactive role by creating an NCS Transition Team, which met regularly with the Office of Homeland Security (OHS) in order to ensure a foundation for a smooth transition. Within the DHS, NCS has been placed in the Information Analysis and Infrastructure Protection Directorate, which is focused on the intelligence analysis aspect of homeland security.

OUTREACH EFFORTS

In other activities, and to leverage collaboration of NS/EP communications, the NCS implemented a Marketing and Outreach Program. The goals of this program are to reach out to potential new NCS members within the Federal Government, raise awareness of NCS accomplishments and current activities within industry and Government, facilitate outreach to State and local government officials and associates, and proactively seek and maintain partnerships with industry forums, associations, and National Security Telecommunications Advisory Committee (NSTAC) member companies.

In support of this program, the NCS provided more than 10 briefings to Government Emergency Telecommunications Service (GETS) users throughout the country, while members of the Wireless Priority Service (WPS) “Tiger Team” actively provided briefings to user organizations to promote the NCS, its products and its services. In addition, the Critical Infrastructure Protection (CIP) Division created its own Outreach Program to promote its “One-Stop Shopping” for emergency communications programs such as GETS, WPS, Telecommunications Service Priority (TSP) and Shared Resources High Frequency Radio (SHARES-HF).

TECHNOLOGY AND PROGRAMS DIVISION

The Technology and Programs Division implements evolutionary NS/EP communications capabilities for a reliable and effective telecommunications infrastructure. The division develops technical studies, analyses, and standards that promote the reliability, security, and interoperability of NS/EP telecommunications.

The division’s objectives stress incorporating advanced, cost-effective technology into NS/EP communications programs. Division personnel evaluate emerging technologies to alleviate impediments to interoperability and to satisfy NS/EP requirements. They use this information as they participate in industry and international standards organization meetings to ensure that NS/EP requirements are incorporated into any recommendations.

The following pages highlight the major projects undertaken by the Technology and Programs Division during FY 2002.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE

BACKGROUND

The OMNCS established GETS to meet White House requirements for a survivable, interoperable, nationwide voice band service for authorized users engaged in NS/EP missions. GETS satisfies these requirements by providing specialized processing in local and long distance public telephone networks. The program ensures GETS users experience a high rate of successful call completion during network congestion or outages arising from natural or manmade disasters. GETS reached full operational capability on September 30, 2001.

From the beginning, GETS planners focused on the public switched network (PSN) as the most efficient, reliable, and robust technology for supporting a service that would meet NS/EP mission requirements. GETS leverages the PSN’s vast resources — a \$300 billion infrastructure with more than 190 million access lines and 26,000 switches. The ubiquitous, robust, and flexible PSN supports more than 90 percent of the Government’s telecommunications needs. Despite its enormous size and complexity, it averages 99.999 percent availability.



The first objective of GETS planners was to expeditiously field a service that would provide priority call treatment. They would then incrementally improve the service with specialized calling features. The strategy of developing GETS by using existing assets of the PSN enabled early implementation and provided technical currency by leveraging the continual improvements made by the industry. Embedding GETS primarily within the software resources of the PSN also made it unnecessary for the Government to purchase, install, maintain, and eventually update network equipment.

The approach to implementing GETS initially focused on the interexchange carrier (IXC) portion of the network. This resulted in separate GETS contracts with AT&T, MCI WorldCom (now WorldCom), and Sprint, the three largest IXCs. They are the only IXCs that can authenticate and process GETS calls. As such, access to these carriers must be available at all PSN end offices. Although the IXCs began with the same basic set of functional requirements, the implementation approach pursued by each IXC and the inherent differences in the structure of the IXCs' respective networks caused the operational features and capabilities to differ slightly among the providers.

After the IXC implementation, the focus of feature development shifted to the local exchange carrier (LEC) networks. The NCS awarded DynCorp (formerly GTE Government Systems Division) the integration contract for development and implementation of GETS features in the LECs and for overall GETS operation, administration, maintenance, and provisioning services. Advanced intelligent network (AIN) technology provided the basis for the first phase of GETS LEC feature deployment, which is alternate carrier routing (ACR). ACR enhances access by automatically attempting all three GETS IXCs.

The GETS integration contractor (IC) entered into contracts with four primary switch manufacturers — Lucent Technologies, Nortel Networks, AG Communications Systems (AGCS), and Siemens — for the implementation of priority treatment and enhanced routing features on their products. The GETS IC also contracted with LECs to deploy and operate these features. During FY 2001, feature deployment continued in the LECs on switches. As of September 30, 2001, all Nortel, Lucent, AGCS, and Siemens switches running software supporting GETS features in LECs under subcontract to the IC had GETS features activated. GETS features will be deployed on additional switches as they are upgraded to required software releases or as additional LECs are brought under contract.

Thanks to proposals submitted by switch vendors leveraging LEC feature development, the GETS Program is deploying enhancements that will help GETS calls terminate from the PSN to customer premises (such as private branch exchanges [PBX]). These enhancements also simplify carrier provisioning of GETS features.

As the PSN evolves into packet-based technology to support voice traffic, the GETS Program Management Office (PMO) is working with industry to maximize and protect the NS/EP community's substantial investment in circuit-switched network enhancements. This work includes one-on-one meetings with carriers and vendors to gain an understanding of their network evolution plans, participation in standards bodies influencing how NS/EP calls may be processed in packet networks, and development of requirements related to packet-based call processing in acquisition packages for the IC and IXC follow-on contracts scheduled for 2003.

OPERATIONS AND FEATURES

Access to GETS is quick and simple: users dial a universal access number using common telephone equipment, such as a standard desk set, secure telephone (such as Secure Telephone Unit-Third Generation), facsimile, or modem. Telephones on the Federal Telecommunications System 2001 (FTS), the Diplomatic Telecommunications Service, and the Defense Information Systems Network (DISN) also provide access to GETS.

When a user dials a GETS access number, a tone prompts for a personal identification number, then a voice recording asks for a destination telephone number. If the access control system is inoperative, a fail open feature allows users to complete their GETS calls. The utility of this feature was demonstrated during the September 11, 2001, attacks on America.

In addition to implementing priority treatment and enhanced routing features in the IXC and LEC trunk networks, the OMNCS has worked to ensure NS/EP calls receive priority in the Signaling System 7 (SS7) networks that manage calls in the carrier trunk networks. In 1993, the American National Standards Institute (ANSI) approved the High Probability of Completion (HPC) Standard ANSI T1.631-1993, which provides a classmark for NS/EP-related signaling messages. ANSI reaffirmed this standard in December 1999. The classmark allows NS/EP calls to be recognized in any U.S. network, facilitating the application of available GETS features.

In 1996, ANSI modified the SS7 standards so that NS/EP traffic would have a higher signaling priority level than regular or non-priority telephone traffic. The GETS Program worked closely with the Network Interconnection Interoperability Forum (NIIF) to facilitate industry migration to the standard related to SS7 message priority. GETS representatives worked with the GETS interexchange and local exchange carriers as well as the switch vendors to reach consensus on a migration plan and

schedule. Their work resulted in the adoption of the Initial Address Message (IAM) Implementation Plan, which was brought to the NIIF.

In December 1997, NIIF accepted Issue No. 0095, Implementing plain old telephone service (POTS) IAM Priority Level 0. On the basis of the resolution, all participants submitted plans, providing specific dates indicating when they will comply with the standard. Switches that comply with the standard serve more than 90 percent of the access lines in the Nation.

INTEROPERABILITY

Many of the significant challenges facing GETS stem from interoperation with other networks and service providers. The GETS PMO is working with industry to ensure consistent, toll-free treatment for service users at privately owned user-to-network access devices. The GETS PMO also is working in concert with the General Services Administration to provide FTS2001 users with improved priority for on-net GETS calls and priority access to the PSN for GETS off-net calls.

Like other services, GETS must navigate the new services-rich, but highly competitive, telecommunications environment spawned by the Telecommunications Act of 1996. Resulting industry deregulation has led to a significant increase in the number of service providers. This environment has given rise to difficulties in placing successful toll-free GETS calls from privately owned point-of-exchange devices, such as coin telephones and PBXs, in some service areas. Previous testing shows these problems to be particularly prevalent for coin telephones owned and operated by small businesses and PBXs operated by the hospitality industry (hotels and motels). Commonly encountered problems include the need to deposit coins at a coin telephone before dialing, improper charging by hotel and motel billing systems, and the inaccessibility of GETS IXCs because of business arrangements between user-to-network device owners and IXCs.

In addition, the OMNCS is working with coin telephone industry groups, such as the American Public Communications Council and hospitality industry organizations and associations, to raise awareness of GETS as an emergency, toll-free service to be given treatment similar to that provided for 911 emergency, toll-free calls.

SUCCESSSES

GETS was one of the first communications services to be used following the terrorist attacks. Despite the heavy telephone congestion occurring immediately following the September 11 attacks and during the first week, 95 percent of the 4,000 GETS calls to and from Manhattan successfully got through. Another 3,000 GETS calls were made in Arlington, Virginia, during the same time period with similar success rates. From the date of the attack until September 28, over 1,000 GETS cards were issued to qualified emergency personnel. During that 17-day span, over 1,500 people made GETS calls.

In the past year, the GETS Program has continued to make significant progress in its outreach efforts to all levels of government (Federal, State, and local) and NS/EP qualifying industry organizations. By the end of FY 2001, there were increases at the Federal (39,639 to 49,052), State (5,927 to 6,986), local (4,780 to 7,955), and industry (2,308 to 4,540) levels in the number of GETS cards issued. Total holdings rose from 52,654 to 68,533.

With the current trend toward more personal and professional wireless communications, more individuals are carrying wireless phones. When the terrorists struck New York and Arlington, wireless phone traffic — like traditional phone lines — became congested. Yet unlike traditional phone lines, emergency responders were less likely to complete GETS calls through wireless communications because wireless networks did not provide priority treatment. Up until this time, the GETS program was not funded to provide priority access for wireless communications.

WIRELESS PRIORITY SERVICE

Reacting to the events of September 11, 2001, the National Security Council (NSC) issued the following guidance¹ to the OMNCS:

- Implement an immediate solution to the cellular radio channel congestion problem, targeted within 60 days, using a readily and commercially available capability for the Washington, DC, area and recommend whether to expand this immediate solution to other metropolitan areas.
- Develop and deploy a priority access queuing system for wireless nationwide, targeted within one year.

This triggered the development of two efforts to combat the wireless priority access problem:

- Immediate — a solution using commercially available and readily implemented technology for a limited geographic area.
- Nationwide — geared to the development of a long-term, nationally available solution.

BACKGROUND

Early in 1995, the OMNCS initiated efforts to develop and implement a nationwide cellular priority access capability in support of NS/EP telecommunications. The OMNCS pursued a number of activities to improve wireless call completion during times of network congestion. In 1998 and 1999, the GETS Program worked with an industry switch vendor to demonstrate end-to-end wireless priority features. The OMNCS also explored the possibility of a national-level database for wireless priority access in 2001.

As a result of a petition from the NCS in October 1995, the Federal Communications Commission (FCC) released a Report and Order (R&O) [FCC-00-242, July 13, 2000] on wireless Priority Access Service (PAS). The R&O offers Federal liability relief for NS/EP wireless carriers if the service is implemented in accordance with uniform operating procedures.

¹ Minutes from the October 5, 2001, meeting on Selected NS/EP Telecommunications Projects, October 9, 2001

The FCC made PAS voluntary, found it to be in the public interest, and defined five priority levels for NS/EP calls.

Wireless network congestion was widespread on September 11, 2001. With wireless traffic demand estimated at up to 10 times normal in the affected areas and double nationwide, the need for wireless priority service became a critical and urgent requirement.

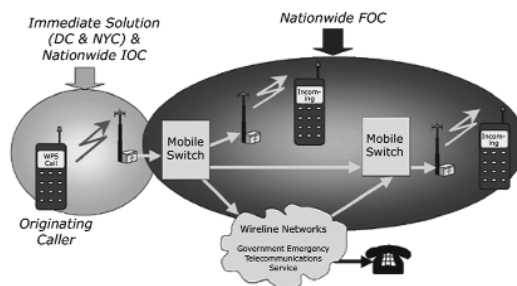
IMMEDIATE WPS

With the White House guidance in October 2001, the NCS began immediate acquisition of priority wireless service for the Washington metropolitan area and recommended and proceeded with services for New York City as well. The February 2002 Olympics in Salt Lake City, Utah, also warranted immediate service. The GETS IC entered into subcontracts with the Immediate WPS service providers, VoiceStream (now T-Mobile) and Globalstar.

The NCS provided Globalstar satellite phones to quickly field the Immediate WPS in the Salt Lake City area during the Olympics. Globalstar made additional satellite capacity available and redirected Utah calls directly to a U.S.-based Earth station. Globalstar also increased landline trunking at the Earth station for GETS calls. These satellite phones were collected after the Olympics for redistribution in Washington and New York, where the service is supplementing a limited WPS capability provided by T-Mobile.

T-Mobile uses the Global System for Mobile (GSM) communications wireless technology and has capitalized on an existing GSM feature called enhanced Multi-Level Precedence and Preemption (eMLPP). During congestion, this feature allows the emergency call to queue for the next available radio channel, without preempting any calls in progress. This immediate capability required an FCC waiver

WPS IMMEDIATE SOLUTION AND THE PLANNED NATIONWIDE CAPABILITY



for T-Mobile because it did not conform to the R&O requirement to invoke the priority service on a call-by-call basis. This means that all calls using authorized Immediate WPS phones receive priority service.

T-Mobile's limited capability became operational during May 2002 in Washington and New York, and mobile phones were distributed by the NCS to those who qualified. By mid-August, T-Mobile supported 1,546 WPS users in Washington and 707 in New York, for a total of 2,253 cellular users. Globalstar also supported 767 of these T-Mobile customers and an additional 639 WPS users without cellular services.

NATIONWIDE WPS

Nationwide WPS is a more comprehensive wireless priority capability. The nationwide initial operational capability (IOC) will consist of priority radio channel access at call origination, similar to the immediate solution but satisfy all the requirements of the FCC R&O, including invocation of the service on a call-by-call basis by dialing a WPS prefix at the start of each NS/EP call. A full, end-to-end capability — beginning with the NS/EP wireless caller, through the wireless networks, through the IXC and/or LEC networks, and to the wireless or wireline called party — will be realized by the nationwide full operational capability (FOC). This service will offer increased probability of call completion during times of widespread network congestion.

Nationwide IOC software development began in July 2002, and installation of this software in commercial mobile radio service provider network switches will start in December 2002. The GETS IC has contracted with several wireless switch vendors (including Ericsson, Nokia, and Nortel Networks) to include the IOC priority capability features in their switches on an expedited schedule outside of their normal software development cycles. Nationwide FOC is planned for implementation by December 2003.

NATIONWIDE INDUSTRY REQUIREMENTS

The nationwide WPS capability is based on wireless standards and industry requirements (IR) documents. The active and cooperative participation of all stakeholders, including major wireless equipment vendors and service providers, successfully produced these IR documents. IOC requirements were completed in February 2002, only 4 months after direction was received from the White House. The FOC requirements will be defined by early fall 2002 to allow the switch vendors to include WPS capabilities in the next software development cycle.

The NCS has also taken steps to ensure that use of the Nation's cellular telecommunication networks by NS/EP personnel does not hinder public use during emergency events. The FCC issued guidelines for NS/EP use of wireless networks, and only NS/EP leadership and key personnel will be approved to use WPS. For those critical individuals who need it, WPS will be a powerful new emergency communications asset and an important national resource.

PRIORITY SERVICES TEAM

Whereas current NS/EP telecommunications services have been designed around the circuit-switched infrastructure of the Public Switched Telephone Network, evolving converged and next generation networks (NGN) are being planned around a packet-switched infrastructure.

As technology evolves, it is increasingly clear that support for emergency telecommunications services (ETS) needs to be included in the developing standards. Third generation and beyond wireless networks as well as packet-switched networks, such as the Internet and the developing Internet Protocol (IP) cable networks, are becoming increasingly more vital to the NS/EP community. Priority Services Team personnel are working with a number of national and international telecommunications industry standards organizations to ensure that evolving standards continue to support ETS.

ETS is a multidimensional initiative addressing standards development work related to network protocols and signaling systems. The ETS initiative was developed to ensure that developing standards continue to support priority for emergency telecommunications regardless of the network topology. Some of the areas being addressed by ETS are: priority establishment, priority access, dynamic restoration, authentication, security, integrity, and management of emergency telecommunications in converging networks and the NGN.

Technology and Programs Division personnel actively participate, sometimes holding leadership positions, in the work of various industry standards development organizations including:

- Telecommunications Committee T1
- Telecommunications Industry Association (TIA)
- International Telecommunication Union, Telecommunications Sector (ITU-T)
- Internet Engineering Task Force (IETF)
- TeleManagement Forum
- European Telecommunications Standardization Institute (ETSI) project known as Telecommunication and Internet Protocol Harmonization over Networks

- Third Generation Partnership Project (3GPP)
- Third Generation Partnership Project 2 (3GPP2)
- TIA/ETSI project Mobile Broadband for Emergency and Safety Applications

Having established the functional requirements for NS/EP services in the aforementioned standards organizations, work is now focusing on technical solutions.

NS/EP COMMUNICATIONS OVER THE INTERNET

The OMNCS continues to assess the potential impact of packet-based technologies on current NS/EP telecommunications services such as the GETS and the TSP Program. The assessment focus is twofold: (1) the period of time commonly referred to as convergence and (2) the evolving NGN. With respect to NS/EP telecommunications, the term convergence refers to the merging of traditional circuit-switched networks with packet-switched networks as they, along with wireless, cable, satellite, and other networks, evolve into an NGN.

Recent studies concluded that few, if any, critical NS/EP telecommunications rely on networks using IP; however, this is likely to change as carriers augment their circuit-switched infrastructure with packet-switched networks using IP to support their voice, video, and data services. Both GETS and TSP were designed around the circuit-switched infrastructure of the public network (PN), so the introduction of packet-switched technologies could adversely affect their continued relevancy. The OMNCS is actively participating in various telecommunications standards bodies, including the IETF and the ITU, to ensure that support for NS/EP telecommunications is continued as packet-switched and circuit-switched technologies converge.



OMNCS efforts have led to the formation of the Internet Emergency Preparedness working group under the auspices of the IETF. The working group is developing a Best Common Practice document or what is commonly known in the IETF community as a Request For Comments (RFC) or set of RFCs for the operational implementation of NS/EP services using existing and evolving Internet protocols.

Similarly, OMNCS personnel have raised the topic of emergency telecommunications to a high level within the ITU; the work program in the ITU is referred to as ETS. Work under ETS will focus on the use and provisioning of the international telecommunications infrastructure for emergency recovery operations for all types of disaster events. This work

encompasses both the period of convergence and the evolution to the NGN.

NETWORK DESIGN AND ANALYSIS CAPABILITY

As directed by Executive Order (E.O.) 12472, the NCS evaluates the ability of the Nation's telecommunications resources to meet NS/EP requirements. Because the NS/EP community relies heavily on the PSN, the NCS developed the Network Design and Analysis Capability (NDAC) to analyze current U.S. networks and to evaluate the need for additional capabilities. The NCS has invested many years in establishing strong working relationships with commercial carriers and Government agencies, and in developing PSN modeling methodologies, tool sets, and unique databases that include proprietary data from the major carriers. The NDAC is used to conduct studies that cover multiple communications areas, such as wireline, wireless, and the Internet. Two of these studies, the Backup Dial Tone (BDT) and Internet Service Provider (ISP), are in response to a tasking from the NSC.

The BDT study uses NDAC to examine methods and technology approaches to enhance the communications reliability in the Washington metropolitan area under emergency conditions. This effort is in response to executive branch concerns that key federal agencies and emergency responders may be at risk of losing essential wireline communications services under disaster or emergency conditions similar to those of September 11, 2001.

Although NS/EP communications have long been supported by the PSN, an increasing number of Government users are now using services offered through the Internet. Additionally, the circuit-switched architecture of the PSN is converging with the packet-switched technology of the Internet, soon evolving into the NGN. Consequently, the logical and physical infrastructures of the Internet must be modeled to support NS/EP analyses.

With the ongoing NDAC expansion to include packet-switched networks, the NCS is developing an Internet modeling capability that will capture the physical and logical interdependencies between ISPs from both architectural and traffic perspectives. The ISP study will use this capability to determine the reliance of NS/EP services on the assets and configuration of the Internet's infrastructure.

ADVANCED INTELLIGENT NETWORK

The AIN is a rapidly evolving telecommunications technology identified by the NSTAC and OMNCS as potentially able to meet the NS/EP telecommunications needs of NCS member organizations.

AIN technology supports the telecommunications architecture consisting of signaling systems, switches, computer processors, databases, and transmission media. The convergence of these elements allows for customized software-defined network services that can be flexibly, rapidly, and cost-effectively configured to meet changing customer needs. Among other capabilities, AIN provides priority recognition, user authentication, enhanced routing, and network management alternatives in support of NS/EP contingency operations.

PN carriers are becoming increasingly dependent on AIN capabilities to deliver services to their customers. Carriers are using AIN to deploy local number portability (LNP), as mandated by the FCC, to open networks to competitive service providers and meet customer demand for new service capabilities, such as mobility, data, and Internet access.

The AIN efforts in the OMNCS address technology applications for NS/EP with the following mission objectives:

- Assess AIN architectures, standards, and implementations
- Define, develop, and demonstrate AIN NS/EP applications
- Ensure NS/EP requirements influence AIN as it evolves
- Facilitate integration into Government initiatives (GETS, DISN, etc.)
- Evaluate AIN security, survivability, reliability, and interoperability

The OMNCS coordinates with NCS member organizations and industry to fulfill mission objectives and identify preliminary services that the OMNCS can introduce into NS/EP initiatives through successful proof-of-concept demonstrations. The OMNCS is deploying AIN-based alternate carrier routing to support LEC-enhanced routing. In conjunction with AIN efforts, the GETS Program Office is pursuing use of the SS7-based HPC ANSI standard for further enhancements.

Intelligent network capabilities have become common in the public telecommunications network. The industry's deployment of LNP service promises to bring near-universal AIN availability. The OMNCS continues to monitor FCC regulations that may affect AIN availability and participates in industry forums to communicate NS/EP needs. Currently the OMNCS is evaluating the role of traditional intelligent network capabilities in emerging multimedia networks, intelligent devices, and future applications of the emerging wireless intelligent network. This applied research

enables the AIN program to influence these exciting new technologies in the developmental stages and ensure the continued efficacy of existing and future intelligent network applications.

INTERNET MONITORING FRAMEWORK

Although the mission of the NCS has traditionally centered on the telecommunications infrastructure of the U.S., the borderless nature of the Internet has put the NCS in a position where it must concern itself with network behavior on a global basis. Awareness worldwide is essential, but the focus remains on North America.

The Internet Monitoring Framework effort is a result of White House direction to develop an Internet situational awareness capability in anticipation of further and more intense cyber attacks. During FY 2001, the NCS prototyped two tools, the Internet Anomaly Reporting System (IARS) and the Attack Early Warning System (AEWS). IARS takes network-to-network performance (latency) data as input, and allows querying, trending, and alerting on that data. AEWS analyzes Border Gateway Protocol traffic to detect when IP address ranges (prefixes) are announced by autonomous systems other than those that usually originate those prefixes. During the coming fiscal year, the NCS will build on this work, developing enhanced prototype tools for visualizing and displaying Internet activity and an integration framework for incorporating other data sources and tools.

FEDERAL WIRELESS USERS FORUM

The Federal Wireless Users Forum (FWUF) is an association of individual Federal Government wireless users. In 1992, the OMNCS established the FWUF as a mechanism for interaction and exchange of information among wireless communications service vendors and users for the purpose of establishing industrywide standards for emerging wireless digital technologies. The objectives of the FWUF are:

- Educate Government users about wireless telecommunications
- Identify the telecommunication needs of Government user
- Facilitate information exchange with other user groups, standards organizations, manufacturers, and service providers to ensure that Government user needs are met and
- Support the interoperability of emerging wireless services and equipment through increased participation in the formulation of Federal policy, support of standardization efforts, and other appropriate activities.

The forum is chaired by the OMNCS and the National Security Agency, and is directed by a steering committee consisting of members from the Department of Defense (DOD), the Department of Commerce, the National Security Agency, the Department of Treasury, the National Institute of Standards and Technology, and the Federal law enforcement community. FWUF holds biannual forums to bring together people from Government and the wireless telecom industry. The activities of the Forum include:

- Multi-day workshops with industry participation
- Outreach work sessions with a focus on a particular user community
- Development of user application profiles.

WORKSHOP HIGHLIGHTS

The 16th FWUF workshop took place from September 11-13, 2001, in San Diego, California. The first day of the workshop was overshadowed by the terrorist attacks at the World Trade Center in New York City, the Pentagon, and Somerset County, Pennsylvania. These events directly affected the FWUF workshop, since many of the attendees represented the military and public safety

communities. This tragedy underscored the critical need for wireless communications to be available and secure for national security and emergency response situations.

The workshop was held in conjunction with the Cellular Telecommunications and Internet Association (CTIA) Wireless Information Technology (IT) and Internet 2001 convention in an effort to gain more exposure among commercial wireless service providers and developers. The workshop participants benefited from demonstrations of the latest in wireless data services and technologies and the future direction of the wireless industry. Participants agreed upon the importance of advancing security and interoperability in wireless communications.

The May 14-16, 2002, workshop in Philadelphia focused on the changes that September 11 had brought upon the Federal telecommunications landscape. Presentations focused on the impact the terrorist attacks of September 11 had in the area of wireless communications and highlighted how imperative it is for both the Federal Industry and Government to work together in continuing the development of an interoperable and secure nationwide Federal wireless communications system. With the ongoing threat to our Nation's security, wireless communications are more important than ever. Once again, the need for interoperability and cooperation among Agencies has been brought to the forefront.

FEDERAL TELECOMMUNICATIONS STANDARDS COMMITTEE

The Federal Telecommunications Standards Committee (FTSC), chaired by the Chief, Technology and Programs Division, OMNCS, continued to develop Federal Telecommunications Recommendations (FTR) to meet specific Government NS/EP requirements. The most recent FTR approved by the FTSC is FTR1080B-2002: Video Teleconferencing Services. FTR development is based on evolving commercial standards and comments

from Government, industry, and the public. The committee forwards all proposed standards through the Manager, NCS, to the GSA or the National Institute for Standards and Technology, as applicable, for approval and publication.

CRITICAL INFRASTRUCTURE PROTECTION DIVISION

In February 2002, the OMNCS Operations Division was restructured and renamed as the CIP Division. The division includes four branches: the Operations Branch; the Planning, Training, and Exercise (PT&E) Branch; the Operational Analysis (OA) Branch; and the IT Branch. A division resource coordinator position and a CIP project coordinator position were established with responsibility for managing and coordinating special projects and programs in the areas of budget, contracting, personnel/resources and project management. These positions report directly to the Chief, CIP Division.

The Operations Branch is responsible for response operations, information sharing activities, and priority telecommunications. The branch coordinates emergency response operations in all-hazards environments. This activity includes activating and staffing emergency operations teams, producing and maintaining standard operating procedures, developing and maintaining fly-away kits for use during response operations, and maintaining the readiness of the National Coordinating Center for Telecommunications (NCC) Operations Center and NCC and OMNCS relocation sites. The branch is also responsible for the day-to-day operations of the NCC and the Telecom-Information Sharing and Analysis Center (ISAC).

The PT&E Branch develops, conducts, and participates in NS/EP and CIP-related national, regional, and organizational exercises and operational training to ensure OMNCS staff and NCS member organizations are prepared to

conduct essential emergency response telecommunications functions. The branch supports several interagency working groups focused on emergency response, continuity of operations (COOP), and continuity of Government planning. With the increased emphasis on critical infrastructure protection, the CIP Division established a division outreach coordinator in the PT&E Branch. This position is responsible for developing and maintaining an integrated outreach strategy to build relationships between the OMNCS and its customers in industry and Government.

The Operational Analysis Branch develops telecommunications infrastructure performance and vulnerability analyses, developing assessments of threats posed to NS/EP telecommunications, manages NDAC functions supporting OMNCS operations, and produces assessments and data supporting operational information sharing and warning.

The IT Branch is responsible for provides policy, guidance, and technical support for OMNCS IT. This includes IT acquisition, policy, and DOD security compliance and technical support in the development and fielding of operational tools, systems, and networks.

NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS

The NCC continues to serve as the operations focal point for the initiation, coordination, restoration, and reconstitution of NS/EP communications services and facilities under all conditions of crises or emergency.

One of the NCC’s major FY 2002 activities was the continuing response to the terrorist attacks of September 11, 2001. The NCC supported emergency operations in lower Manhattan, coordinated response efforts between the Federal Government and telecommunications service providers and vendors, participated in Federal, State, and local interagency restoration teleconferences, and provided significant TSP and GETS support.

To capture what had been learned during response operations in Manhattan and at the Pentagon, the NCC prepared an after action report assessing its September 11 response activities and developed recommendations for future operational improvements. This assessment identified significant activities needed to enhance NCC capabilities, including:

- Upgrades to the facilities, and technical and communications capabilities at the NCC and at NCS relocation sites
- Updates to operational procedures incorporating lessons learned
- Augmentation of the organizational structure, skill sets, and training of NCC response elements and
- Development of improved methods to enhance information management within the NCC emergency operations teams and other OMNCS response elements.

Other major NCC activities in FY 2002 included:

- Broadening membership to include additional nontraditional service providers and equipment manufacturers. Development and implementation of additional strategies to further encourage new membership to the NCC and Telecom-ISAC were initiated and continue. The following companies joined the NCC during FY 2002; Avici, Boeing, Cingular, CTIA, Lucent, and VeriSign. Raytheon and Motorola joined the Telecom-ISAC function of the NCC.
- Continued staffing of the 24/7 NCS Watch Desk in the DOD’s Global Network and Security Operations Center to foster the sharing of information with industry and coordinate information sharing among Government Network Operations Centers. Enhanced procedures to ensure effective information sharing with critical partners,

such as other ISACs, Federal Computer Incident Response Center, and the National Infrastructure Protection Center.

- Continuing to maintain an effective working relationship on telecommunications issues with both the Canadian Government and the telecommunications industry in Canada. In January and September 2002, the Manager, NCC co-chaired meetings of the U.S./Canada Civil Emergency Preparedness Telecommunications Advisory Committee (CEPTAC). Additionally, the Canadian Federal Government has identified personnel from Industry Canada and the Office of Critical Infrastructure Protection and Emergency Preparedness to be deployed to the NCC to coordinate response efforts that require U.S./Canada cooperation.
- Establishing a bilateral relationship with Mexico, to foster the creation of a CEPTAC between U.S. and Mexico, and eventually a tri-lateral body to work critical telecommunications infrastructure cross border issues.

TELECOM-INFORMATION SHARING AND ANALYSIS CENTER

The Telecom-ISAC function is an integral function of the NCC that builds on the existing NCC membership, procedures, and trust relations to facilitate voluntary collaboration and information sharing among 24 industry member companies and between the industry and Government. As with the rest of the NCC, the ISAC area of interest covers all hazards, although the ISAC core business focuses on cyber issues and threats.

In response to the September 2001 terrorist attacks, the one-person, 8 hour-a-day, 7 day-a-week trial watch function went immediately to a 24/7 operation supporting the Telecom-ISAC and NCC and has remained at that level. During FY 2002, the Telecom-ISAC watch and analysis operation experienced rapid growth in activity and visibility due to its critical role. Its importance will continue given the increasing

sophistication of the value-added technical and liaison services provided by the on-site watch and analysis team.

Opportunities for liaison and collaboration between the Telecom-ISAC analysts and other industry and Government watch centers increased dramatically and contributed significantly to critical infrastructure protection efforts. The NCC Watch liaison function continues to expand and includes operational relationships with Canadian Government entities. It also provided significant support to the Cyber Interagency Working Group established by the NSC in the wake of disclosure of vulnerabilities in the Simple Network Management Protocol (SNMP) to recommend improvements in the Federal Government's ability to respond to future incidents.

During FY 2001 the Telecom-ISAC began efforts to add an analysis capability. A watch daily analysis network was established to assist watch analysts in daily research into Internet exploits to help mitigate impending or ongoing cyber events. The Telecom-ISAC also prepared the NCS response to a tasking by the President's CIP Board on the feasibility of creating a Global Early Warning Information System (GEWIS) to provide a worldwide Internet health monitoring function.

GLOBAL EARLY WARNING INFORMATION SYSTEM

In March 2002 the President's CIP Board tasked the NCS to evaluate the feasibility of creating a GEWIS of cyber attacks on critical national infrastructures using sensor data currently available from the private sector. The NCS's response to the board in July 2002 stated that GEWIS is feasible and that work already begun by the Telecom-ISAC in support of the Cyber Warning Information Network (CWIN) provided a strong base upon which to build such a capability. The target GEWIS would be capable of acquiring relevant data, managing that data through recognized knowledge management processes, analyzing and monitoring the data to

determine potential threats and malicious activities, and finally, creating actionable, early warning information for dissemination to both industry and Government entities responsible for critical infrastructure protection. The recommended approach is to build on the Telecom-ISAC base infrastructure and processes. The requirements analysis phase for the GEWIS, began in FY 2002 and culminated in the System Requirements Review in September 2002.

ALERTING AND COORDINATION NETWORK

Prior to January 1, 2001, the National Telecommunications Alliance (NTA) managed and operated the Alerting and Coordinating Network (ACN) — a switched, private line network — to provide emergency communications among the Regional Bell Operating Companies, their suppliers, and certain Government agencies. The ACN is not dependent on the PSN so it can provide continued communications during disruptions, congestion, and outages affecting the PSN. When NTA dissolved on January 1, 2001, the ACN was in jeopardy of being disbanded. Because the ACN provides emergency backup communications capability that could help coordinate response to and recovery from a widespread network outage, the Director, Office of Science and Technology, directed the NCS to acquire the assets and provide operational support to ensure the continued viability of the ACN.

Operational responsibility for the ACN has been incorporated into the NCC operations to serve as a vital coordination resource in the event of severe congestion or catastrophic damage to the PN. The OMNCS is working with industry to establish procedures for maintaining and utilizing the ACN and expanding its availability within the telecommunications infrastructure. The ACN can also provide for cross infrastructure coordination in the event of outages in the telecommunications infrastructure affecting other infrastructures or outages in other infrastructures affecting

telecommunications. The OMNCS will be seeking participants from other infrastructures to allow this capability to be realized.

Major changes were initiated in FY 2002 to upgrade the ACN to a Voice over IP (VoIP) network. Conversion of existing ACN connections began in FY 2002 and will be completed in early FY 2003.

CYBER WARNING INFORMATION NETWORK

In a memorandum dated May 30, 2001, from the National Coordinator for Security, Infrastructure Protection and Counter-terrorism, NSC, the NCS was tasked with planning and executing the deployment and operational management of the CWIN. The CWIN development effort is designed to facilitate the immediate sharing of critical cyber information within Government and with its industry partners.

Since the inception of the CWIN, operational capabilities and procedures have been implemented over an existing network at seven Federal watch centers, which are located at five geographically dispersed locations. Beginning in mid-FY 2002, NCC began deployment of a dedicated network to support CWIN operations at these 7 Federal watch centers and an additional 75 centers to include cyber operational elements of the Government, private corporations, and ISACs.

NORTH ATLANTIC TREATY ORGANIZATION CIVIL COMMUNICATIONS PLANNING COMMITTEE

The OMNCS represents the U.S. on the North Atlantic Treaty Organization (NATO) Civil Communications Planning Committee (CCPC), its telecommunications working group, and other subsidiary bodies. The Department of State (DOS) detailee to the OMNCS is the head of the delegation. CCPC purview extends to telecommunications and postal services. The OMNCS accordingly consults closely with U.S.

telecommunications service providers and affected U.S. Government agencies and organizations. During FY 2002, the CCPC met twice in plenary session: once at NATO headquarters in Brussels, Belgium, and the other in Tallinn, Estonia. Its telecommunications working group met four times, and the postal working group met twice. An ad hoc working group tasked to develop a paper on risks and threats to civil communications met three times.

Shortly after September 11, 2001, Article 5 of the NATO treaty was invoked for the first time ever, resulting in the 19 permanent member nations and 27 partner nations of the CCPC modifying and intensifying their work programs. The focus of activity is on elimination and/or mitigation of acts of terrorism within the 46 NATO and partner nations.

Major CCPC FY 2002 activities and accomplishments were as follows:

- Approved the 2002 CCPC Work Program based upon Ministerial Guidance. The program includes civil support for alliance military operations, support for civil emergency planning, protection of the civil population against weapons of mass destruction, and cooperation with partner nations.
- Cooperated with Canada in the development of a CCPC Web site located in Vancouver.
- Participated in a NATO Crisis Management Exercise (CMX-2002).
- Presented to the committee an analysis of lessons learned from the anthrax contamination in the U.S. Postal System.
- Presented to the committee an analysis on lessons learned from the attack on the World Trade Center, including reconstruction of major telecommunications nodes and the restoration of voice/data service to Wall Street. Also examined infrastructure

interdependencies and the “cascade” effect of infrastructure overload and failure during major incidents.

- Completed an analysis delineating risks and threats to civil communications within NATO countries.
- Developed and distributed a questionnaire to 46 nations regarding the legal mechanisms in place to support NATO during periods of Article 5 activities as well as non-Article 5 situations.
- Participated in a seminar held in Estonia to examine how civil communications can support national emergency preparedness in a demanding environment.
- Completed an analysis on the use of cellular systems for crisis and civil emergencies.

In April 2002 a new CCPC U.S. industry representative (Qwest) was selected to replace the outgoing industry representative (BellSouth).

CRITICAL INFRASTRUCTURE PROTECTION — INTERNATIONAL OUTREACH

On October 8, 2001, the President signed E.O. 13231 establishing the “President’s Critical Infrastructure Protection Board.” Various subgroups were then formed under this board. On January 9, 2002, the first meeting of the CIP Standing Subcommittee on International Affairs was held at the DOS. The Subcommittee includes 10 Government agencies, including the NCS.

The OMNCS participated in the following bilateral discussions to gain international cooperation for protection of critical infrastructures:

- Belgium, April 1-2: A delegation from Brussels led by the advisor to the Belgian Minister for Telecommunications met in Washington with various Government

agencies, including the NCS. The Deputy Manager proposed possible arrangements between the U.S. and Belgium to share information on computer viruses.

- United Kingdom, April 14-18: A high-level delegation from the United Kingdom headed by a director of British Telecom and including the manager of Her Majesty's Office of e-Envoy visited the U.S. under the auspices of the OMNCS. The delegation visited Ground Zero in New York City and was briefed by senior executives from Verizon. This was followed by briefings at the NCS by Government employees and industry representatives. Further site visits and briefings were held at Ashburn, Virginia (AT&T), the DOS, the Federal Emergency Management Agency (FEMA), and the Pentagon.
- India, April 29-30: OMNCS representatives traveled to New Delhi to attend bilateral discussions. Industry-Government participation was stressed as a model for information sharing. The Deputy Manager, NCS, issued a formal invitation to high-ranking members of the Indian Government to visit the NCS for briefings and training sessions.
- Italy, May 2-3: OMNCS representatives traveled to Rome to attend bilateral discussions and a conference. Lessons learned from 9/11 were presented to a large audience to include Italian cabinet ministers and the U.S. Ambassador.
- Japan, June 13-14: A high-level Japanese delegation headed by a cabinet counselor visited Washington for bilateral discussions on civil infrastructure protection. Formal meetings were held at the DOS on June 13. On June 14, the Japanese delegation visited the NCS for telecommunications-specific briefings. Welcomed by the Manager, NCS, the delegation received briefings and a tour of the facilities by the Deputy Manager and his staff.

- Mexico, June 18-19: Bilateral discussions were held in Mexico City. The OHS headed the U.S. delegation that included OMNCS representatives. Following the official talks, the OMNCS representatives met with senior representatives from major Mexican telecommunications companies to discuss possible information sharing arrangements and Government-industry cooperation.
- Canada: Bilateral discussions with Canadian Government officials in Ottawa were held in August.

STANDING SUBCOMMITTEE ON UPGRADES

Under the authority of three Presidential Directives and one E.O., the Deputy Manager of the NCS serves as Chair of the Standing Subcommittee on Upgrades (SSU), an interagency group of experts responsible for "hotline" operations. The group has the following mandates:

- Convene as necessary to set technical parameters and establish overall milestone schedules for upgrade enhancements, to assign engineering and procurement responsibility, and to review milestone achievements.
- Provide guidance and direction to, and approve composition of, the U.S. Technical Experts Delegation, and approve scheduling, agendas, and U.S. positions for bilateral and/or multilateral meetings on technical matters relating to Government-to-Government communications links.
- Keep the NSC informed, as appropriate, of the activities of the SSU and U.S. Technical Experts, and request NSC guidance on non-technical (policy) matters as appropriate.

The Deputy Manager of the NCS served as Deputy Head of Delegation to the U.S.-Russia Meeting of Technical Experts held in Moscow October 22-26, 2001. Subsequent to the

Moscow talks, the Deputy Manager held SSU meetings during December 2001 and April 2002 to reach interagency consensus on hotline modernization plans. Another meeting of the U.S.-Russia Technical Experts meeting was held at the DOS in October 2002.

TELECOMMUNICATIONS SERVICE PRIORITY PROGRAM

The TSP Program, established by an FCC R&O dated November 17, 1988, provides a regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications services. The FCC authorizes and requires service vendors to provision and restore services with TSP assignments before services without such assignments. FY 2002 TSP activities included:

TSP OPERATIONS

The OMNCS facilitated coordination between industry and Government to ensure adherence to TSP responsibilities within the evolving telecommunications marketplace and national security/emergency preparedness environment. Working closely with the TSP Oversight Committee (OC), the OMNCS examined the TSP Program in the context of its operational homeland security role. In the wake of the September 11, 2001, terrorist attacks, TSP Provisioning and Restoration requests tripled. This increase was attributable to OMNCS critical infrastructure rebuilding efforts, the ongoing war on terrorism, and growing awareness of the importance of business continuity practices.

During FY 2002, the OMNCS issued 568 provisioning TSPs and 9,650 restoration TSPs. The user base grew by 72 organizations with the greatest increase in requests coming from the financial sector and State and local governments. Military departments continue to be one of the largest users of the TSP Program as well.

The OMNCS facilitated meetings of the TSP OC, which identifies, reviews, and recommends actions to correct or prevent systemic problems in the TSP Program. With this committee, the OMNCS focused its efforts on several operational TSP issues, including difficulties in the areas of broadband provisioning, and policies and procedures implemented by the Defense Information Technology Contracting Office to provision DOD TSP requests.

To assist in the additional workload of requests originating from the financial sector in the wake of the attacks, the Federal Reserve Board has detailed a representative to the NCS to help ensure a more uniform and streamlined process for granting TSP requests between the program office and the financial sector.

TSP INFORMATION TECHNOLOGY SOLUTIONS

The OMNCS continues to recognize the importance of IT solutions for improving TSP processes. During FY 2002, the NCS's Office of Priority Telecommunications IT efforts focused on database integrity issues of the Priority Telecommunications System (PTS), the information system used to support TSP provisioning and restoration. They also devised and implemented a number of features to improve PTS functionality and usability.

Throughout FY 2002, the TSP Web site (<http://tsp.ncs.gov>) was regularly enhanced and revised to distribute crucial TSP Program information to existing and potential TSP clients. The site includes instructions for using the PTS and e-forms applications, which offer an easy, secure, and universal mechanism for performing various TSP processes.

TSP OUTREACH STRATEGY

In addition to conducting outreach efforts to new telecommunications service providers, educating and training emergency responders about the TSP Program remained an OMNCS priority. Due to the growth of inquiries about the TSP Program and increased participation from new

user groups following the September 11 attacks, the OMNCS placed emphasis on reaching State and local NS/EP personnel, first responders, and private sector entities sponsored by Federal agencies (e.g., financial institutions). To that end, the OMNCS provided comprehensive TSP training to potential vendors, Federal, State, and local users, and emergency response coordinators. Public and private entities, including the Financial and Banking Information Infrastructure Committee, the Veterans Administration, the Transportation Security Administration, and the American Petroleum Institute, were briefed and/or trained on TSP processes.

NETWORK SECURITY INFORMATION EXCHANGE ACTIVITIES

The joint meetings of the NSTAC and Government Network Security Information Exchanges (NSIE) provide a trusted environment in which industry and Government representatives can exchange information on threats to and vulnerabilities of the PN. The NSIEs focus on technical issues affecting the security of the PN, such as unauthorized penetration or manipulation of the PN software, databases, and other infrastructures supporting NS/EP telecommunications services.

The NSIEs exchange ideas on technologies and techniques for addressing and mitigating the risks to the PN and its supporting infrastructures. In FY 2002, the NSIEs held several ad hoc sessions to discuss security technologies and their implementation, including SNMP and telecommunications operating system security. The Security Requirements Working Group (SRWG) was formed by the NSIEs as an outgrowth of a discussion on the security of systems that control the network. The SRWG drafted the document "Operations, Administration, Maintenance, & Provisioning Security Requirements For Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane," providing requirements that will allow

vendors, Government agencies, and service providers to implement a secure telecommunications network management infrastructure. The document will be provided to standards bodies for adoption.

In FY 2002, the NSIEs completed their 2002 PN risk assessment. It was determined that vulnerabilities introduced by rapid technological advances and the dynamic business environment have made it increasingly difficult to protect against intrusions. Additionally, the PN's pervasiveness and the value of information flowing over its networks make it a primary target for attacks. These factors suggest that the overall risk to the PN continues to grow.

SHARED RESOURCES HIGH FREQUENCY RADIO PROGRAM

The SHARES-HF Radio Program continues to provide emergency communications in support of all-hazards situations and special operations. SHARES-HF incorporates the resources of 1,054 HF radio stations contributed by 92 Federal, State, and industry organizations into a nationwide emergency message-handling network.

During FY 2002, SHARES-HF conducted 103 on-air operations. Following the September 11 disaster operations, 342 SHARES-HF stations, representing 37 Federal, State, and industry organizations, generated the largest number of station availability reports since SHARES-HF was established in 1989. Additionally, the longest continuing Level 2 Special Operation was conducted to support the State of the Union address, Super Bowl XXXVI, and the Winter Olympics.

Readiness continued to be emphasized. Seven hundred sixty-two SHARES-HF stations, representing a 21 percent increase over the preceding year, participated in three nationwide readiness exercises conducted during the year. The SHARES-HF Interoperability Working Group, a permanent body established under the NCS Council of Representatives (COR),

continued to meet bi-monthly to coordinate SHARES-HF network activities and to address issues affecting interoperability of Federal HF radio systems. The working group, composed of 142 members representing 98 organizations, published the 11th edition of NCS Handbook 3-3-1, SHARES-HF Directory; continued to expand the digital and Automatic Link Establishment structure of the nationwide SHARES-HF Coordination Network; and continued to support new HF technologies. The working group also continued to expand awareness of SHARES-HF throughout the Federal emergency preparedness community through the SHARES-HF Outreach Program.

On August 30, 2002, the NCS provided an HF capability to the OHS by transferring and installing HF radios and antennas at the OHS.

PLANNING, TRAINING, AND EXERCISE SUPPORT

The PT&E Branch is responsible for ensuring a cadre of skilled civilian and military reservist personnel are qualified and ready to provide emergency response support during crises and emergencies. To meet this goal, the PT&E Branch sponsors a nationwide training program through:

- Emergency Response Training (ERT) seminars
- Internal and external exercises
- Regional planning support
- OMNCS Augmentee Program
- Division Outreach Program.

TRAINING

The PT&E Branch trains the telecommunications industry, OMNCS staff, NCS Regional Managers, Emergency Support Function (ESF)-2 support personnel, military reservists, and regional and State emergency

responders to effectively execute their responsibilities during the various phases of response and recovery operations. During FY 2002, the branch successfully coordinated and performed the following activities:

ERT SEMINARS

ERT seminars are a highly visible and successful training program for the NCS. These seminars are 2 day events designed to provide industry, Federal, regional, State, and local personnel with the background and information required to successfully respond to a crisis situation. The ERT Program is in its third phase, in which more than 700 attendees have participated in sessions in 10 of the 12 Federal regions. During FY 2002, the OMNCS conducted seminars in Seattle, Washington (Northwest Arctic Region), Honolulu, Hawaii (Pacific Region), and Framingham, Massachusetts (Northeast Region).

In response to the attacks of September 11, 2001, the ERT Program revised its training curriculum to include new and emerging threats, such as the effects of terrorism on communications. Today, the program provides participants with an understanding of communications issues associated with these threats, including the increased demands on networks and personnel, and the best use of finite industry and Government resources. Since the training program started in 1993, more than 2,100 attendees have participated in 33 sessions. This program continues to receive recognition for improving the ESF-2 response and recovery structure.

TELECOMMUNICATIONS SUPPORT FOR THE 2002 WINTER OLYMPICS GAMES

Due to a heightened concern for security and the need for a prompt response to any emergencies during the 2002 Winter Olympics in Salt Lake City, Utah, FEMA activated the response capabilities of the Federal Response Plan. Federal agencies, which had assigned responsibilities for the ESFs, were tasked to

provide staff and resources at an initial operating facility located at the Camp Williams National Guard Facility approximately 30 miles south of Salt Lake City. The NCS, as Lead Agency for ESF-2 (Communications) provided an on-site team led by the NCS Regional Manager from Federal Region VIII with support from five U.S. Army Reserve officers from the NCS Individual Mobilization Augmentee unit. The team was on-site from January 30 through March 1, 2002.

In the absence of an actual emergency, the ESF-2 team participated in training scenarios with the assembled Federal and State emergency responders. These training events provided opportunities to demonstrate the NCS's telecommunications resources supporting emergency response operations. The team also supported the deployment of GLOBALSTAR satellite telephones to Federal, State, and local emergency managers. The satellite telephones provided alternative communications links that could bypass local wireless call congestion. Additionally, GETS cards were distributed to give the emergency responders prioritized call-completion on the wireline services.

EXERCISES

The OMNCS conducts internal and external exercises to maintain expert knowledge of, and proficiency in, the management, integration, and employment of NS/EP telecommunications resources. In FY 2002, the CIP Division, PT&E Branch, deferred conducting exercises to allow resources to be focused on operational issues that evolved after September 11.

OMNCS AUGMENTEE PROGRAM

The OMNCS continues its Augmentee Program, which is supported through the Department of the Army's Individual Mobilization Augmentee (IMA) Program. The augmentees supplement existing staff within the OMNCS and at regional locations to support ESF-2 and NCS Regional Managers during national emergency operations and disaster response planning.

IMA PROGRAM

The NCS IMA Program provides a valuable array of skilled Reserve personnel to augment telecommunications response activities. During Presidentially declared disasters, the IMA Program provides the NCS with a surge capability to deploy and react to myriad situations associated with ESF-2 operations. IMA personnel are often among the first Federal disaster response personnel to reach a disaster scene. Many of these reserve officers are telecommunications professionals in their full-time civilian careers and are able to apply their skills when responding to Federal emergencies. The IMA Program continues to provide an extremely important and invaluable service to the OMNCS NS/EP mission at the national and regional levels.

The IMA Program broadens OMNCS presence in the 10 Federal Regions. The program is responsive to NCS Regional Managers when they are fulfilling their emergency planning duties. During annual training and drills, augmentees participate in a variety of planning and training opportunities for ESF-2 that support Regional Manager emergency telecommunications responsibilities. The program meets mission responsibilities through deployment of IMAs using a combination of annual training, paid and nonpaid individual drills, and temporary tours of active duty. The NCS provides a minimum of one annual 2-week training period for each of its IMAs. Paid drill participation for the IMAs is 100 percent.

During FY 2002, the NCS Augmentees provided over 158 duty days to support contingency and disaster relief operations. Augmentees were deployed in New York City and at the NCC to provide assistance after the September 11 disaster. Additionally, a team deployed to Camp Williams, Utah, to provide contingency communications support during the 2002 Winter Olympics in Salt Lake City. Deploying to support NCS Regional Managers during disaster response, such as hurricane and flood response and recovery, the NCS Augmentees are an integral element of the OMNCS, supporting critical operations in the NCC and the field.

CONTINUITY OF OPERATIONS

The OMNCS maintains an active and robust COOP program that ensures its essential functions will be sustained throughout any emergency. As directed by E.O. 12656, "Assignment of Emergency Preparedness Responsibilities," the NCS developed the COOP Program in 1990 to identify essential missions and functions that must be performed in any emergency, developed plans to perform these missions and functions, and developed the capability to execute those plans.

During FY 2002, the OMNCS revised the COOP Program to reflect additional functional requirements and new Federal emergency preparedness guidance. This guidance includes Presidential Decision Directive 67, "Enduring Constitutional Government and Continuity of Government Operations," and "Federal Preparedness Circular 65, Federal Executive Branch Continuity of Operations." The NCS is an active member of the interagency COOP Working Group, chaired by FEMA. This forum coordinates and develops Federal COOP policies and initiatives. Through its involvement in the COOP Working Group during FY 2002, the NCS continues to play an important role in developing emerging Federal emergency preparedness requirements associated with alternative operating facilities and tests, training, and exercises. The NCS is co-chairing an interoperable COOP communications Sub-Group that is responsible for developing a Federal Preparedness Circular that will provide guidance to the Federal Government on Interoperable COOP Communications' issues.

During FY 2002, the OMNCS continues to enhance its COOP capability by continually upgrading its two emergency relocation sites. As integral elements of a viable COOP capability, these sites will continue to provide an effective operating environment to support OMNCS critical mission functions if the NCS Headquarters is unavailable.

CIP DIVISION OUTREACH

During FY 2002, a division outreach coordinator position was established as part of the division's critical outreach strategy to ensure that all CIP-related activities and programs are properly coordinated and fully integrated within the CIP Division, the OMNCS, and throughout industry and Government. A coordinated outreach effort is necessary to keep the division at the forefront of national CIP efforts. As part of the outreach strategy during FY 2002, the coordinator began developing the CIP Outreach Plan. The plan involves coordinating several outreach efforts, including briefings, training, and staffing information booths; and developing fact sheets and brochures, that communicate information regarding CIP programs. The latest information product, dated July 2002, describes the WPS Program and the application process.

OPERATIONAL ANALYSIS

The Operational Analysis (OA) Branch was established as part of the new CIP Division to serve as the focal point for developing analytical assessments of physical and cyber threats to, and network vulnerabilities of, the PN affecting NS/EP telecommunications. Analytical studies conducted during this fiscal year include:

Analysis of International Submarine Cable Vulnerabilities —February 2002. The Special Advisor to the President on Cybersecurity tasked the NCS to conduct a vulnerability analysis of the International Submarine Cable System. Specifically, the analysis was to investigate the submarine fiber optic cables with landing points in the U.S.; determine the degree to which these cables are concentrated in a few switching centers; investigate current security measures for protecting these assets; conduct an impact analysis to determine what would happen if one or more of these assets were damaged; and provide recommendations for improving diversity and security of the system. Research indicated that although there are areas for improvement, overall, the architecture supporting international communications is very robust and diverse. Specific findings and recommendations are in the final report dated June 2002.

Physical Security of Cyber Assets — April 2002. The NCS was tasked by the President's CIP Board, Committee on Physical Security to conduct a baseline security assessment of key physical assets that support the national information systems infrastructure. The analysis included identification of the major telephony and Internet facilities within the U.S., an assessment of the impact of the loss of these facilities, an assessment of current security practices, and recommendations for security and diversity enhancements. In addition, a preliminary crossings analysis was conducted, which identifies where concentrations of major national telephony and Internet backbone fiber optic cables converge on physical crossings, such as tunnels and bridges. Specific findings and recommendations will be incorporated into the final CIP Board's Physical Security Committee report.

Canada-Mexico Border Crossings — April 2002. The OHS Policy Coordinating Committee tasked the NCS to conduct a security analysis of the telecommunication assets critical to communications among the U.S., Mexico, and Canada. This information was generated to support bilateral discussions with Canada and Mexico in regard to the joint protection of critical infrastructures. The objectives of these discussions are to develop a common CIP framework, identify cross-border equities, and discuss ways to eliminate/mitigate vulnerabilities.

WorldCom Insolvency Analysis — June 2002. The NCS conducted an analysis of the WorldCom insolvency situation to understand how WorldCom's current situation, or potential future deteriorated situation, could affect NS/EP telecommunications services. The analysis centers on identifying the economic and technical implications of WorldCom insolvency and developing a broad spectrum of potential outcomes.

INFORMATION TECHNOLOGY SUPPORT

The IT Branch is responsible for ensuring that information systems enhance the performance and operational readiness of OMNCS personnel. These information systems encompass a range of capabilities, from Defense Information Systems Agency (DISA) local area networks (LAN) to laptops, distributed over a variety of facilities including headquarters, alternative facilities, and remote users.

As DISA-LAN liaison, the IT Branch represented OMNCS interests in such areas as the proposed network enhancements, the migration to Defense Message System e-mail, and implementation of new user authentication including the deployment of client Public Key Infrastructure. In addition, the branch considered the impact to operations resulting from network changes, such as the temporary closure of port 80 on gateways due to the NIMDA worm.

The IT Branch also serves as a focal point for information security issues. Activities over the last year have included ensuring that the system administrators of NCS systems were aware and had taken the proper measures to protect against the 65 plus advisories, bulletins, and technical notices originating from DOD and countless vendor bulletins. It also assisted in guiding systems such as the Watch Desk Analysis and the Test and Analysis Lab toward certification under the guidelines established for the DOD Information Technology Security Certification and Accreditation Process. The IT Branch assessed system exposure to vulnerabilities, such as the recently published SNMP vulnerabilities, and defended systems against compromise by establishing security policies, constant administration, and hardening of equipment ranging from laptops to networks.

The IT Branch focused on improving capabilities available to users. To improve the effectiveness of personnel, the IT Branch reviewed current

network, hardware, and software needs and identified, procured, and implemented solutions. These equipment and connectivity solutions were implemented at headquarters, alternative locations, and remote users to improve the robustness of operations.

PLANS AND RESOURCES DIVISION

The Plans and Resources Division provides centralized management and oversight to the OMNCS for acquisition matters, financial matters, strategic and performance management planning activities, staffing allocations, and other personnel-related matters. The Plans and Resources Division exercises authority and ensures accountability over all resources allocated to NCS programs.

The Division serves as the interface with the DISA directorates on financial and acquisition matters; DOD Planning, Programming, and Budgeting System (PPBS) documentation and execution; and acquisition management. The division also conducts analyses and makes recommendations to the OMNCS and the DISA directorates on the optimal use of NCS resources to support mission requirements consistent with statutory and policy constraints.

PLANNING

The Planning Team documents the OMNCS leadership's near-, mid-, and long-term strategic direction, vision, and priorities through the development of the Strategic Plan, Business Plan, Performance Plan, Future Years Corporate Plan, and Advanced Acquisition Plan.

The Planning Team, through the implementation of the Strategic and Performance Plans, comprehensively evaluates organizational performance and effectiveness. The OMNCS developed the NCS Strategic and Performance Plans in response to the requirements of the Government Performance and Results Act

(GPRA) of 1993. These plans embrace the GPRA concept of engaging in a cycle of strategic planning, performance planning, and evaluation of an organization's effectiveness.

After collecting performance metric data during 1999, the OMNCS reviewed and reassessed its performance measurements based on changes to the external environment and its own reorganization. The Plans and Resources Division revised the Performance Plan and the Strategic Plan in FY 1999. These documents defined the new strategic goals and performance measures of the NCS, which reflected an increased emphasis on customer service.

FINANCIAL MANAGEMENT

The Financial Team provides the overall fiscal direction to the OMNCS for day-to-day operations. The Financial Team develops and produces all PPBS-related documentation for the OMNCS, including documentation for program objective memorandums, budget estimates, the President's budget submissions, and all related exhibits. The team ensures that exhibits reflect decisions and directions from the Manager, NCS, and DOD.

The Financial Team also leads in developing, coordinating, and implementing funding procedures as directed and provides guidance and assistance to non-DOD agencies involved in the NCS to ensure that their requirements are met. In addition, the team provides fund citations, ensuring the availability of funds and compliance with fiscal laws, regulations, and policies.

ACQUISITION MANAGEMENT

The Acquisition Team provides OMNCS divisions support throughout all aspects of the agency-level acquisition process. This includes preparing acquisition plans, statements of work, contract solicitations, proposal evaluations, and other acquisition support documentation for OMNCS programs and projects. The Acquisition Team also monitors contractual compliance, identifies contractor deficiencies,

recommends contractual remedies, tracks contract expenditures, monitors all contractor reporting for accuracy, and recommends adjustments.

**CUSTOMER SERVICE
DIVISION**

The Customer Service Division serves as the primary conduit between the NCS and both member and non-member organizations and coordinates interaction of NCS program activities among the divisions. This coordination ensures that the technical and operating divisions are properly supported. The primary functions of the Division are to support the Committee for National Security and Emergency Preparedness Communications (NS/EPC), its related COR, and the President’s NSTAC. The following sections describe the Customer Service Division activities for FY 2002.

**THE COMMITTEE FOR NATIONAL
SECURITY AND EMERGENCY
PREPAREDNESS COMMUNICATIONS AND
COUNCIL OF REPRESENTATIVES**

The NS/EPC is an interagency group providing advice and recommendations on national security and emergency preparedness, including representatives from 22 Federal departments and agencies. The group was formerly the Committee of Principals, but was renamed the NS/EPC earlier this year when it was designated as one of the standing committees of the CIP Board.

In October 2001, the President issued E.O. 13231, “Critical Infrastructure Protection in the Information Age” to support the President’s ability to “ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.”

E.O. 13231 established the President’s CIP Board to coordinate all Federal activities and programs that relate to protecting information systems and networks supporting critical infrastructures, including:

- Federal departments and agencies
- Private sector companies which operate critical infrastructures
- State and local governments’ critical infrastructures and
- Related national security programs.

Lt Gen Harry D. Raduege, Jr., as the Manager of the NCS, is a member of the CIP Board and serves with other senior Government officials from the executive branch and other Federal agencies. In addition, General Raduege is also a member of the Board’s Coordination Committee. E.O. 13231 also assigned to the Manager, NCS the responsibility of chairing the NS/EPC.

In January 2002, at the first meeting of the NS/EPC, the committee developed an NS/EPC mission statement: “To assist the President, the National Security Council, the Director of the Office of Science and Technology Policy, the Director of the Office of Management and Budget, and the Assistant to the President for Homeland Security, in coordinating national security and emergency preparedness communications policies, programs, and services, including proposing and implementing improvements.” The committee also approved new bylaws and established a work plan as requested by the CIP Board.

During FY 2002, the NS/EPC met four times and considered taskings received from the CIP Board. Specific tasks included evaluating the need for a backup dial tone capability, emergency notification alert program, and cyber security. In each case, the NS/EPC considered the NCS studies and provided recommendations



Daniel P. Burnham (left), Chairman, President, and Chief Executive Officer of Raytheon Company and Chair of the President's National Security Telecommunication Advisory Committee (NSTAC), addresses NSTAC Principals and senior Government and telecommunications industry officials during the NSTAC Business Session, held March 13 in the State Department's Loy Henderson Auditorium. Beside Burnham is Lieutenant General Harry D. Raduege, Jr., Manager of the National Communications System. (Photo by Robert Flores, Defense Information Systems Agency.)



Secretary of State Colin Powell, addresses the Principals of the President's National Security Telecommunications Advisory Committee, during the Business Session, held on March 13 at the State Department. (Photo by Robert Flores, Defense Information Systems Agency.)

that were incorporated into the NCS response to the CIP Board tasking. On the question of cyber security, the NS/EPC agreed that a global early warning system of cyber attack activity should be established using the NCC as a core site for GEWIS.

In other projects, the NS/EPC considered the NCS responses to the President's Special Adviser for Cyberspace Security to assess the vulnerabilities of submarine cables, telecom hotels, and points of peering for Internet service providers and cross-border telecommunications facility vulnerabilities.

The COR met three times in FY 2002 and established several working groups to assist it in carrying out its responsibilities. The COR established a working group on the emergency notification service strategy (requested by the CIP Board) and on the national strategy to secure Cyber Space to assist the COR and NCS in formulating its recommendations. In addition, the COR established a working group on critical facilities to assist department and agencies in addressing the numerous issues concerning the identification and safeguarding of critical telecommunications facilities.

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

In FY 2002, the President's NSTAC continued to provide industry-based advice and expertise on issues related to the implementation of NS/EP communications policy. The NSTAC members and the entities they represent are committed to this partnership in support of NS/EP on behalf of the U.S. Issues addressed by the NSTAC and its subgroups included industry and Government information sharing in support of CIP efforts, network convergence, cyber threats to U.S. computer systems, and the National Strategy for Cyberspace Security.

The President's NSTAC held its NSTAC XXV meeting on March 13, 2002, in Washington, DC, at the DOS. The central theme of the meeting was cyberspace security, and it featured remarks from Secretary of State Colin Powell; Senator Robert Bennett of Utah; Mr. Richard Clarke, the President's Special Advisor on Cyberspace Security; and Mr. Howard Schmidt, Vice Chair of the President's CIP Board. Subjects of discussion included the Cyber Agency Working Group, WPS, Router and

Protocol Security, Physical Security of Telecom Networks, the National Infrastructure Simulation and Analysis Center, Wireless Networks of the Future, and the Internet Service Provider's Role in Security. During the Business and Executive Sessions of the meeting, the NSTAC Principals and senior administration officials discussed these and other topics developed by the NSTAC's Industry Executive Subcommittee (IES) during FY 2002.

NSTAC LEADERSHIP

On August 9, 2002, President George W. Bush named Dr. Vance Coffman, Chairman and Chief Executive Officer (CEO) of Lockheed Martin as the NSTAC Chair. Dr. Coffman replaced Mr. Daniel P. Burnham, Chairman and CEO of Raytheon Company. That same day, the President named F. Duane Ackerman, Chairman and CEO of BellSouth Corporation as Vice Chair, replacing former Qwest Chairman and CEO Joseph P. Nacchio.

NSTAC'S INDUSTRY EXECUTIVE SUBCOMMITTEE ACTIVITIES

During FY 2002, the NSTAC's IES continued to identify and develop communications issues for consideration and to direct the activities of its subgroups. The four key issues were network security, the National Plan for Critical Infrastructure assurance, "last mile" (delivery of high bandwidth services to the local level) bandwidth availability, and legislative and regulatory issues.

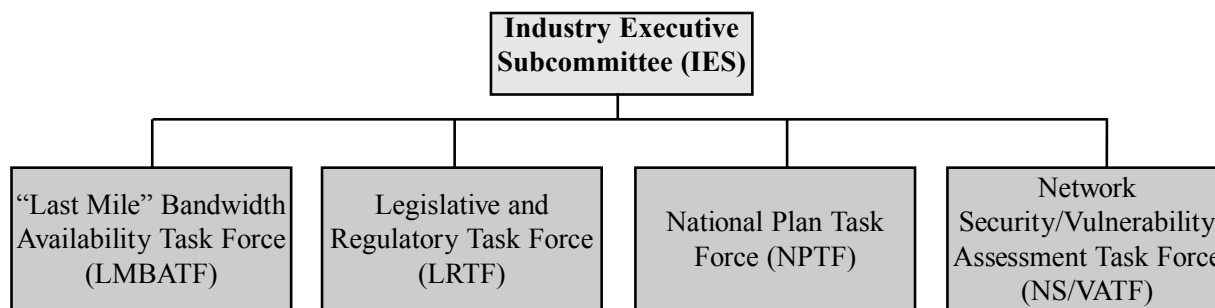
NSTAC'S NETWORK SECURITY/VULNERABILITY ASSESSMENTS TASK FORCE

Following NSTAC XXIV in June 2001, the IES formed the Network Security Vulnerability Assessments Task Force (NSVATF) and charged the group to address PN policy and technical issues related to security and vulnerability of the converged network control space, including wireless, network simulation and testing, standards, and consequence management issues. The group was also charged to analyze specific countermeasures (e.g., functional requirements) needed to address identified vulnerabilities.

In its report published in March 2002, the NSVATF concluded that additional steps were necessary to increase control space security of the evolving PN, including the need to enhance industry and Government cooperation. The NSVATF also encouraged industry and Government support of the NSIEs efforts to develop a cross-industry security posture that could help provide a foundation for protecting the control space of the emerging PN. With regard to wireless networks, the task force concluded that the Government should deploy wireless local area networks with higher levels of security and consider policies that would reduce the risks of using personal area network devices.

Through its analysis, the NSVATF recognized that the PN and its services supporting NS/EP users would continue to be at risk from

The President's National Security Telecommunications Advisory Committee (for the NSTAC XXV Cycle)



increasingly well-coordinated and technologically sophisticated threat sources. Because of this threat environment, the NSVATF concluded that industry and Government should continue participating in ISACs to develop and implement unified capabilities to respond as attacks occur. Moreover, industry and Government must continue working together in devising countermeasures and strategies to help mitigate physical and cyber attack impacts on the PN and other critical infrastructures.

NSTAC'S NATIONAL PLAN TASK FORCE

At the June 6, 2001, NSTAC XXIV meeting, the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism requested the NSTAC's assistance in developing the Bush Administration's National Plan for Critical Infrastructure Assurance. At that meeting, Federal officials also briefed a new national initiative for information sharing and dissemination, the CWIN, as part of the discussion on national information sharing capabilities. The IES formed the National Plan Task Force (NPTF) to discuss the proposed CWIN and develop further input to the National Plan. The NSTAC input to the National Plan — based on the NPTF work — focused on the need for an authoritative, national-level capability to disseminate warnings and facilitate response and mitigation efforts for cyber crises across the Nation's infrastructures. The committee also concluded that key elements of such a capability spanning public and private sectors should include information collection and sharing, information analysis, dissemination of alerts and warnings, and post-event analysis. The assessment input considered the CWIN as a part of that larger national capability.

The NSTAC determined that ISACs should be leveraged by both industry and Government in building a national capability to address cyber crises, and should serve as the Government's primary means of interface with industry. In addition, it determined that industry and Government should develop communications

mechanisms to link the ISACs to each other as well as to Government. The committee also found that Federal departments and agencies should consider alternative means for communicating during emergencies as appropriate within each critical infrastructure sector.

NSTAC'S "LAST MILE" BANDWIDTH AVAILABILITY TASK FORCE

The IES formed the "Last Mile" Bandwidth Availability Task Force (LMBATF) based on the recommendations of the "Last Mile" Bandwidth Availability Scoping Group and a request for NSTAC assistance from Lt Gen Harry D. Raduege, Jr., Manager, NCS, in October 2000. Lt Gen Raduege asked the NSTAC to recommend what the Government could do to expedite the provisioning of last mile bandwidth or to mitigate the provisioning periods for such services.

The LMBATF concluded its analysis of the last mile issue during the NSTAC XXV cycle and presented its findings and recommendations in the March 2002 "Last Mile" Bandwidth Availability Task Force Report at NSTAC XXV. The task force found that the provisioning periods for high-bandwidth services in the last mile are affected by a combination of complex factors including legislative and regulatory activities, the dynamic telecommunications environment, challenging site locations, and the Government's own contracting policies and procedures.

The task force developed specific recommendations on how industry and Government could reduce provisioning time and mitigate the effects of provisioning periods. The recommendations were in three categories: to improve contracting and practices within Government; to urge the Government to establish realistic requirements for its own telecommunications needs; and to better forecast to industry the future bandwidth services it may need.

The task force also studied whether the TSP System can be used to expedite last mile provisioning requests because TSP provisioning assignments are used by the NS/EP community to facilitate the expedited installation of telecommunications circuits that otherwise could not be installed within the required time frame. Although TSP seems to be an applicable solution for many NS/EP last mile bandwidth requests, according to TSP Rules, TSP provisioning assignments can be applied only to services originating from new business requirements, which excludes services associated with the contract transition.

NSTAC'S LEGISLATIVE AND REGULATORY TASK FORCE

During each NSTAC cycle, the Legislative and Regulatory Task Force (LRTF) analyzes the impact of current legislative and regulatory actions on NS/EP communications. In FY 2002, the LRTF played an active role in addressing the implications of two critical issues—convergence and information sharing. Specifically, the LRTF explored whether additional legal authority is required to ensure NS/EP services in the converging and the NGN.

The LRTF concluded in its documentation that until the standards for packet-based services are established and the Government's requirements in the evolving environment are certain, new legislation or regulation is premature. The LRTF also stated that the legal issues underlying the NS/EP priority services provisioning to the Federal Government in an NGN environment are extremely complex and may require further study.

During the NSTAC XXV cycle, the LRTF also continued to address barriers to information sharing such as the Freedom of Information Act (FOIA), liability, and anti-trust. The LRTF monitored pending FOIA legislation from the 106th and 107th Congresses and heard from congressional staff on the status and outlook of this legislation. The NSTAC also participated in correspondence with the President concerning

information sharing legislation. On September 26, 2001, President Bush replied to a letter sent during NSTAC XXIV, saying he supported a narrowly drafted exception to FOIA to protect information about corporations' and other organizations' vulnerabilities to information warfare and malicious hacking. In a December 17, 2001, letter to the President, the NSTAC Chair encouraged the President to continue to support information sharing legislation.

NSTAC'S SEPTEMBER 11 "LESSONS LEARNED" AD HOC GROUP

In response to a request from the Special Advisor to the President for Cyberspace Security, the NSTAC formed the September 11 "Lessons Learned" Ad Hoc Group to provide an industry perspective on lessons learned in responding to the September 11 tragic events. The ad hoc group focused on access procedures at disaster sites, communications procedures, and industry representation within the NCC. In particular, the group noted that at first, industry was denied access to the New York disaster site by law enforcement, causing a delay in service restoration. Based on the ad hoc group's analysis, the NSTAC recommended that standard access control procedures be established across Federal, State, and local government jurisdictions at disaster sites to address this issue.

The group noted that wireless and cell phone services were disrupted due to congestion in the PN, highlighting the need for wireless priority service capability, an idea that the NSTAC originally recommended in 1995.

Additionally, the ad hoc group addressed communications procedures during emergencies. The events of September 11, 2001, demonstrated the need for standard procedures to improve communications among decision makers, operational personnel, and other stakeholders during emergencies. The ad hoc group found that the requisite operational procedures were already developed and in place at the NCC, including procedures related to the NCC's Telecom-ISAC function. Finally, the ad

hoc group concluded that the telecommunications industry should work through NCC representatives to address communications requirements during emergencies.

Deeming Internet services increasingly important to the operations of business and Government agencies as well as disaster response, the ad hoc group examined the mix of industry representation in the NCC. The group found that while NCC members represented the majority of the wireless carrier market share and more than half of the Internet backbone provider market, NCC members represent only a minority of the Internet access provider market. The ad hoc group concluded that augmenting Internet access provider membership in the NCC could help the NCC better address potential network security issues.

As part of its lessons learned analysis, the ad hoc group reviewed previous NSTAC recommendations, recognizing that the NSTAC's cumulative work could provide valuable information related to ensuring reliable infrastructure services and securing the Nation's critical facilities.

OTHER AD HOC GROUPS

NSTAC created several other ad hoc groups in 2002, including one to explore outreach efforts to raise awareness of the NSTAC, and one on cyberspace. The Research & Development (R&D) Exchange Ad Hoc Group, established to schedule and coordinate the fifth NSTAC R&D Exchange, became an official task force in August 2002. The task force will work in conjunction with the White House's Office of Science and Technology Policy and the Georgia Institute of Technology to bring together industry, Government, and academia to discuss R&D issues related to national and homeland security.

NSTAC XXVI ACTIVITIES

As NSTAC task forces proceed with their work in FY 2003, the Presidential committee will continue to provide industry expertise on a range of subjects. Building on its prior work, NSTAC will contribute to the development of the National Strategy to Secure Cyberspace and will analyze the potential need for legislation related to Internet attacks. It will also explore law enforcement issues related to WPS implementation and numerous security issues pertaining to the telecommunications industry. The NSTAC will address issues related to wireless communications as well as the development of policy recommendations for identifying and mitigating the vulnerabilities in pervasive software and protocols across the Internet's infrastructure.

NCS ISSUANCE SYSTEM

The NCS Issuance System, outlined in NCS Directive 1-1 and issued under the authority of E.O 12472 "Assignment of NS/EP Telecommunications Functions," establishes the framework for the internal workings of the NCS. It includes directives, circulars, manuals, handbooks, notices, and OMNCS office orders. The issuance system provides guidance concerning policies, procedures, management, and personnel of the NCS.

PUBLIC AFFAIRS

In the year following the September 11 attacks, NCS received numerous inquiries from the news media concerning emergency telecommunications. These inquiries have come from national media outlets such as the major television networks, national wire services, leading national newspapers, government focused telecommunications magazines, and specialized telecommunications periodicals.

Inquiries have focused on WPS, GETS, and the NCS mission to work with industry in support of emergency communications. Questions have also addressed the TSP, the Telecom-ISAC, and relationships with DOD information systems

organizations, such as the Joint Task Force—Computer Network Operations. The NCS has also received inquiries concerning the DHS and the NCS role in that department.

In addition to fielding press inquiries, the NCS has distributed a variety of publications, reports, fact sheets, and brochures on NCS programs and the President's NSTAC. The publications are provided to the media, telecommunications companies, potential NSTAC membership applicants, and senior Government officials to provide background information on NCS programs and activities.

The NCS published its FY 2001 Report, in late June 2002. The NSTAC Reports for the NSTAC XXV cycle were published in early March 2002 and distributed at the NSTAC XXV meeting held March 13. NCS also published the LMBATF Report and the NS/VATF Report. In addition, NCS is finalizing the NSTAC XXV Issue Review, a recap of all NSTAC issues dating to the committee's creation in 1982, for publication in 2003.

OUTREACH

The Deputy Manager, NCS, has spearheaded an active outreach effort to promote the NCS and its programs to a variety of commercial, Federal, State, local, and international audiences and is supporting OMNCS Division leaders and program managers in doing the same. NCS representatives attend Government and commercial technology symposia, as well as conferences on homeland security, information assurance, and critical infrastructure protection. Since the September 11 attacks, numerous opportunities have arisen for NCS leaders to participate in panel discussions and other public forums to describe NCS and its critical role in homeland security and NS/EP communications.

NS/EP TELECOM NEWS

NS/EP Telecom News, published quarterly by the OMNCS, provides NS/EP information for the NCS and NS/EP telecommunications community, helping the NCS member organizations keep abreast of legislative, regulatory, judicial, technological, and policy developments.

NCS HOME PAGE

The NCS home page (<http://www.ncs.gov>) provides information on the NCS and NSTAC. The home page contains NCS and NSTAC history, information about NCS and NSTAC programs and activities and online versions of NCS and NSTAC publications.

The OMNCS continues redesigning many of its Web pages, including the NCS home page. The redesigns will give NCS Web site visitors better access to sites concerning NCS programs and activities, as well as updated information about NCS activities. The current redesign is also incorporating format changes to make the site accessible to people with disabilities.



V

NS/EP TELECOMMUNICATIONS SUPPORT AND ACTIVITIES OF MEMBER ORGANIZATIONS



The background of the page is a complex collage. At the top, there are several large, stylized 'V' shapes. Below these, there are images of satellite dishes on the left and a globe in the center. To the right of the globe, there is a table of data. The bottom right corner shows a close-up of a cable connector. The overall theme is telecommunications and global connectivity.

20	OVERC
19	OVERC
18	OVERC
17	OVERC
16	OVERC
15	OVERC
14	OVERC
13	OVERC
12	OVERC
11	OVERC



DEPARTMENT OF STATE (DOS)

NS/EP TELECOMMUNICATIONS MISSION

The Department of State's (DOS) mission is to support the President in formulating and executing U.S. foreign policy. This mission determines its telecommunications support requirements. Essential DOS telecommunications functions include the following:

- Implementing and managing a reliable, secure, responsive, survivable, cost- effective, global telecommunications network
- Providing communications support (including data, voice, imagery, facsimile, and video) for all U.S. Government agencies at U.S. overseas diplomatic facilities
- Maintaining a rapid response capability via alternative means to ensure the continual availability of effective communications links under all conditions.

TELECOMMUNICATIONS STAFF ORGANIZATION

DOS manages its telecommunications through the Bureau of Information Resource Management and the Diplomatic Telecommunications Service Program Office.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Information Technology Facilities Consolidation

The DOS continues to consolidate and standardize its enterprise server operations. This project, which commenced in mid-fiscal year (FY) 2001, focuses on developing and implementing a plan for a comprehensive "server farm" concept. This is to establish the infrastructure for consolidating

information technology (IT) facilities and processing resources, such as servers, databases, and applications, into centrally managed facilities and systems. The benefits are savings in staffing and facilities throughout the Department, improved security, data integrity, operational reliability, technical support, and availability.

Interagency Collaboration

OpenNet Plus is designed to address Secretary Powell's commitment to provide DOS employees with access to the Internet's World Wide Web to support the conduct of our foreign policy initiatives. This program is scheduled for completion by April 30, 2003, and will enable secure Internet browsing and Web transaction services via the Department's existing OpenNet (Sensitive But Unclassified) computer network infrastructure. The OpenNet Plus program will bring the Internet to DOS desktops domestically and overseas, improve network security by replacing or enhancing current legacy systems, consolidate information systems, and establish a common operating system.

The Classified Connectivity Program (CCP) will modernize the Department's classified infrastructure by providing classified personal computers, e-mail, CableXpress telegram distribution, and Secret Internet Protocol Router Network (SIPRNET)-Intelink access (the Department of Defense (DOD)/Intelligence community Intranet) at all approved posts by December, 2003. At the end of FY 2002, DOS had installed the CCP at 123 posts.

Secure Voice Program

The Department is actively transitioning its legacy secure voice system to the new National Secure Voice Standard, the Secure Terminal Equipment (STE) system. Funding was designated for this project, and STE systems are being received from the National Security Agency (NSA). The replacement process of the legacy secure voice system with this new technology is proceeding

smoothly. STE units are being deployed both domestically and overseas. Current projections show a complete legacy-secure voice replacement in place by the end of 2003.

Communication Security

Implementation of over-the-air-rekey (OTAR) continues within the DOS. To date, 86 percent of the eligible posts have been converted to OTAR. The Department continues toward its goal of converting all eligible posts to OTAR operations by the end of calendar year (CY) 2002. The implementation of OTAR is enabling the Department to significantly reduce the physical cryptographic keying material at OTAR posts. Communications security is dramatically enhanced by this reduction in cryptographic holdings.

The DOS created a Public Key Infrastructure (PKI) Program Office to implement PKI, providing users secure Internet and Intranet Web application and e-mail services previously unavailable. The program was implemented during FY 2001. In addition to providing public key technology to State users domestically and overseas, the Department is providing this smart card-based access technology to users from the Department of Justice's (DOJ) Immigration and Naturalization Service (INS) to access visa information resources, and to all Federal agencies with requirements to access the Interagency Collaboration Zone at overseas posts. This technology will have a profound impact on the overall level of information security for the DOS and the conduct of its business in the future.

Messaging Systems

On April 4, 2002, the Under Secretary for Management approved a recommendation to accelerate the implementation of a modern messaging system for the DOS. This project, originally scheduled for FY 2006, has been accelerated by 2 years — to be completed in FY 2004.



DEPARTMENT OF STATE (DOS) *continued*

The new system will replace the outmoded cable system and integrate all of the Department's current processes for messaging, including cables, memoranda, and e-mail.

Enterprise Network Management

The Enterprise Network Management (ENM) Program will modernize the Department's data communications capabilities to enhance the diplomatic readiness of the Department. The ability of the Department to advance the foreign policy interests of the U.S., including supporting the overseas roles of the other Federal agencies abroad, depends upon the quality of the communications infrastructure. ENM is currently augmenting the availability of this connectivity by using Virtual Private Network (VPN) technology to create

network "tunnels" through the global Internet infrastructure. These tunnels provide an alternative route capability that is independent of the existing telecommunications infrastructure, thus increasing overall network availability. To date, ENM has implemented about 40 alternative routes using this technology, with plans to implement all posts by FY 2005, thereby achieving a commercial quality network availability of 99.5 percent.

CCP

The CCP started in 1999 to modernize the DOS classified infrastructure, providing employees posted overseas with desktop access to classified e-mail and telegram services, as well as to SIPRNET, a Web-based tool that allows users access to certain intelligence community Web pages. This capability

means closer collaboration among agencies to serve and protect the U.S., its citizens, and its interests worldwide. In addition, CCP will replace obsolete IT and communications hardware and software currently in use by some posts to process classified foreign affairs information. CCP also provides for a consistent architecture across classified and unclassified systems. As a result, there are greater efficiencies with reduced cost through standardization and an improved administrative toolset, allowing Web-enabled configuration management. The system also aligns with e-Government initiatives and the President's management agenda. By the end of deployment, targeted for the end of CY 2003, all eligible overseas posts will have a modernized classified infrastructure fully capable of supporting foreign affairs functions.



DEPARTMENT OF TREASURY(TREAS)

NS/EP TELECOMMUNICATIONS MISSION

The essential functions of the Department of Treasury (TREAS) requiring NS/EP telecommunications are summarized as follows:

- Protecting the President, Vice President, their families, and other dignitaries
- Managing the economic activities of the U.S., including all monetary, credit, and financial systems
- Administering the laws pertaining to customs, taxes, alcohol, tobacco, and firearms
- Serving as the principal economic advisor to the President
- Accomplishing international economic and monetary control as it pertains to the well-being of the Nation
- Manufacturing currency, coins, and stamps, and establishing methods of exchange.

TELECOMMUNICATIONS STAFF ORGANIZATION

TREAS manages telecommunications through the Office of the Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO), under the Assistant Secretary of the Treasury for Management. This office oversees the National Communications System (NCS) liaison and NS/EP support activities and provides management guidance and financial

oversight to improve the Department's use of telecommunications systems. The office is also responsible for ensuring, through the exercise of program management authority, that TREAS bureaus have access to a cost-effective, technologically sound telecommunications infrastructure so that they may carry out their missions.

The Acting Treasury CIO serves as one of two e-Government coordinators for the Federal CIO Council. The Federal CIO Council is the lead interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information services.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Computer Emergency Response Capability

A formal computer emergency response capability was implemented with full-time coverage for the Department. TREAS completed the year with no major embarrassing or operational compromises of its electronic data systems and hopes to continue this trend as well as to enhance the intrusion prevention, detection, and remediation capabilities it now has in place.

Support for the Federal PKI Development

TREAS provided technical and leadership support for the development and use of an interoperable, governmentwide PKI permitting electronic transactions over the Internet in a trusted environment. The Director of Treasury's Office of Information Systems Security served as the chair of the Federal PKI Policy Authority.

Critical Infrastructure Protection

TREAS bureaus participated in the Homeland Security (HLS) workshops used to identify functions, assets, and vulnerabilities in performing critical law enforcement responsibilities. Organizational and/or system interdependencies were also identified. TREAS chartered a Critical Infrastructure Protection (CIP) Working Group composed of bureau CIP officers responsible for ensuring the integration and coordination of policy, planning, and implementation among and within the various bureau security organizations and infrastructure asset owners. TREAS also established a Tools Sub-Working Group to develop and field Network Vulnerability Assessment Tool Kits. This group has evaluated open source and commercial software, determined a core suite, is procuring and configuring hardware, fielding imaging kits, and training users on use.

Public Safety/Law Enforcement Wireless Activities

During 2002, TREAS led significant activities in addressing interoperable wireless communications for public safety and law enforcement officials. TREAS was the initial program manager for the Office of Management and Budget's (OMB) e-Government Wireless Initiative. Project SAFETY Interoperable COMMunications (SAFECOM) was initiated to formally address interoperable wireless communications for public safety agencies at the Federal, State, and local levels. The goal of project SAFECOM is to promote and implement solutions that will allow public safety officials to communicate with each other when necessary. In 2002, TREAS partnered with DOJ to design and implement a joint law enforcement land mobile radio



DEPARTMENT OF TREASURY(TREAS) *continued*

system that will meet the requirements of both Departments. This will yield cost efficiencies and also provide interoperable communications for the two law enforcement agencies. The two Departments are planning a pilot of this joint radio system in early 2003.

Treasury Communications System

The Treasury Communications System (TCS) is the largest privately owned network in the civilian Federal Government and provides critical services to TREAS bureaus and employees. To ensure continuous availability of these critical services, a TCS disaster recovery site was formally established outside the Washington, DC, metropolitan area limits

in FY 2002. This site operates in a “warm standby” mode. If the disaster occurs at the primary TCS operations center, the recovery site will provide uninterrupted critical services to TREAS and its bureaus.

To protect TREAS technology and information assets, the cyber protection mechanisms were enhanced in FY 2002 with the deployment of network intrusion detection systems. These systems are both inward facing to protect against attacks and viruses introduced by the public Internet and outward facing to protect against insider attacks.

The TREAS-wide Directory Services capability was expanded in FY 2002 to

include information relative to all personnel located throughout TREAS and its bureaus. In March 2002, an enterprise PKI Operational Certificate Authority (OCA) system for use by all TREAS bureaus was deployed. The system is capable of issuing PKI certificates to TREAS’ 200,000 users. The TREAS Directory Service structure provides the repository for certificates issued through the TREAS PKI OCA.

To strengthen physical and logical access control to TREAS information assets, the TREAS and six of its bureaus entered into a PKI/smartcard deployment during late FY 2002.



DEPARTMENT OF DEFENSE (DOD)

NS/EP TELECOMMUNICATIONS MISSION

Under the provisions of Executive Order (E.O.) 12472, DOD maintains the following NS/EP telecommunications responsibilities:

- Provide, operate, and maintain the telecommunications services and facilities to support the National Command Authorities and execute the responsibilities by E.O. 12333, "U.S. Intelligence Activities," December 4, 1981.
- Ensure that the Director, NSA, provides the technical support necessary to develop and maintain adequate plans for the security and protection of NS/EP telecommunications.
- Execute the functions listed in Section 3(I) of E.O. 12472.

TELECOMMUNICATIONS STAFF ORGANIZATION

DOD includes the Office of the Secretary of Defense (OSD), the military departments and the services within them, the unified commands, and other agencies established to meet specific U.S. military requirements. The Defense Information Systems Agency (DISA) is a separate DOD agency under the direction, authority, and control of the Assistant Secretary of Defense (ASD) for Command, Control, Communications, and Intelligence (C3I).

The principal staff positions concerned with NS/EP telecommunications in the OSD are the Under Secretary of Defense for Policy and the ASD for C3I. C3 requirements are the concern of the Joint Staff J6.

"POWER TO THE EDGE"

Transformation of the Global Information Grid (GIG)

Excerpted from CHIPS Magazine article by Dr. Margaret Myers, Principal Director, Deputy CIO, DOD

"The two truly transforming things, conceivably, might be in information technology and information operation and networking and connecting things in ways that they function totally differently than they had previously. And if that's possible, what I just said, that possibly the single-most transforming thing in our force will not be a weapon system, but a set of interconnections and a substantially enhanced capability because of that awareness."

*Secretary of Defense Donald H. Rumsfeld
– August 9, 2001*

Defense Transformation

The Secretary of Defense's words indicate how the transformation from today's platform-centric environment to tomorrow's network-centric environment will create an information advantage. By increasing richness and reach simultaneously, net-centricity allows us to interconnect our arsenal of advanced and extraordinarily capable combat and intelligence platforms and provide them with timely and accurate data. Net-centricity allows users to augment data available from their own systems and capabilities with data from other locations and other sources well removed from the normal sensor range of the platform itself. In the net-centric environment, global information and local data sources will be fused to provide what we call "power to the edge."

Transformation of the DOD Enterprise

It is critical to ensure that transformation of the DOD be viewed as an enterprise

endeavor and implemented in a balanced way. We must provide capabilities to both the warfighting operations that are core to DOD and the important business operations, such as financial management and logistics support of our forces. What we are trying to achieve with net-centricity is an information environment—the GIG—where people will fully utilize the a trusted network, and where their performance will not be limited solely by the capabilities under their direct command, but rather they will benefit from the global reach of the network and all the other capabilities that will be interconnected by that network. The GIG will provide users the edge they need to prevail in any circumstance—business or warfighting.

IT Enabling Transformation

The critical leg of this transformation is the ability to be truly synchronized in both time and place. If one examines the tactics that al Qaeda used on September 11, one will see that they operated asynchronously. Their operatives did not come together in any significant numbers until just before the attack. Achievement of effective information flow and coordination did not require the total force to be exposed at any one specific time. They stayed dispersed and hidden until the time to execute their mission. That is in essence what we are trying to do with our forces when they operate net-centrically. When we achieve net-centricity or the ability to operate asynchronously in time and place, we will be as stealthy as al Qaeda, but with a bigger punch.

High Leverage Net-Centric Investments

The Secretary is pursuing high leverage net-centric investments representing three of the major tipping points for achieving transformation. Although these investments are part of an integrated GIG



DEPARTMENT OF DEFENSE (DOD) *continued*

strategy, they are designed to meet separate, but related GIG objectives. The first pillar, the GIG bandwidth expansion, provides networked services with unprecedented bandwidth to operating forces as well as intelligence, surveillance, and reconnaissance assets that can be interconnected by increasingly available fiber optics. Advanced Wideband Satellite Communications extends these capabilities through wireless tails of

incredible bandwidth — also using optical technologies. Providing the actual power to the edge falls to the third of the net-centricity pillars — horizontal fusion. This pillar, will allow us to post our data to the network, pull other data from the same network, and make sense out of it all.

Power to the Edge

Clearly, the transformation for net-centricity in the Department is well on its way. We will proceed at a brisk pace to

increase the power to the edge, whether it's in the form of the ability to hold many targets at risk with a global net-centric surveillance targeting capability or with the ability to automatically tag selected censored data. As the capabilities improve, the ability to network applications through fiber optics and forward-deployed satellite communications will proceed rapidly.



DEPARTMENT OF JUSTICE (DOJ)

NS/EP TELECOMMUNICATIONS MISSION

The NS/EP telecommunications mission for the DOJ is to provide telecommunications facilities and services in support of DOJ NS/EP essential functions. The Department centralizes its NS/EP responsibilities in the Justice Management Division for all Department entities except the Federal Bureau of Investigation (FBI), which maintains separate secure network facilities.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Director, Telecommunications Services Staff (TSS) operates and manages DOJ's consolidated data transport network, law enforcement message processing systems, and Telecommunications Services Center. TSS also provides networking and technical assistance to DOJ's offices, boards, divisions, and bureaus. Secure interagency message transmission is offered through separate facilities.

The Information Security Policy Group (ISPG), Security and Emergency Planning Staff is responsible for security oversight of all national security communications systems within the Department. The ISPG is the central office of record for all national security information applicable to the Department.

The Drug Enforcement Administration (DEA), FBI, INS, and U.S. Marshals Service (USMS) continue to administer their own communications security programs.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The following current/ongoing DOJ activities support NS/EP objectives:

- TSS provides representation for DOJ on the Committee for National Security and Emergency Preparedness Communications (NS/EPC).
- TSS provides representation for DOJ on the Council of Representatives (COR).

- A TSS representative serves as the Chairman of the Telecommunications Service Priority (TSP) Oversight Committee.
- DOJ continues its active participation in the NCS activities of the NS/EPC/COR, and participates in NCS NS/EP telecommunications support, activities, and programs.
- DOJ continues its vigorous support of the activities of NCS NS/EP planning, program, and contingency programs, and emerging NS/EP telecommunications programs. DOJ has sponsored full access for three commercial companies that are either departmental component contractors or companies engaged in NS/EP support in their normal duties.
- Additionally, the Department is an active participant in the Government Emergency Telecommunications Service (GETS) Program, the TSP Program, the SHARED RESOURCES High Frequency Radio Program (SHARES-HF), and the Wireless Priority Service (WPS).

SIGNIFICANT ACCOMPLISHMENTS

- As a result of the events of September 11, 2001, the Department has undertaken an effort to familiarize departmental components with the GETS and WPS programs and to enlist the participation of those organizations with identified NS/EP roles.
- Since its creation in 1998, the Justice Consolidated Network (JCN) has brought more than 1,000 departmental component office locations on-net supporting more than 4,000 "Permanent Virtual Circuits," ranging in rate from 64 kilobits per second (Kbps) to 5 megabits per second (Mbps).
- This network, a consolidation of more than 20 individual systems, was implemented to facilitate the interconnection and interoperation of organizations such as the DEA, FBI, INS, USMS, and U.S. attorneys' offices, as well as the many other Justice organizations with law enforcement and litigation missions. Most departmental components have now transitioned to the JCN with the latest, the Executive Office for Immigration Review, now 100 percent on-net and the USMS partially cutover.
- In addition, during 2002 connectivity for the U.S. Attorneys' and INS was reengineered to support system upgrades. Services are currently being upgraded to augment the DEA's increased data rate requirements. For 2003, in addition to completing the U.S. Marshals' transition, DOJ projects implementing some degree of support for video and Voice over Internet Protocol (VoIP) traffic.



DEPARTMENT OF THE INTERIOR (DOI)

NS/EP TELECOMMUNICATIONS MISSION

The Department of Interior's (DOI) mission is to efficiently manage the Nation's natural resources. The DOI and the U.S. Department of Agriculture (USDA) co-manage the National Interagency Fire Center in Boise, Idaho. It is the Nation's primary emergency support facility for forest fire suppression. DOI provides emergency transportable land mobile radio (LMR) systems from multiple radio caches strategically located throughout the U.S. to support wildland fire fighting and other national emergency activities. Forest fire suppression operations are conducted in close cooperation with State and local government emergency support activities.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Telecommunications Systems Division of the office of the CIO is responsible for DOI telecommunications

program management. Bureau telecommunications managers and their staff are responsible for telephony, radio, and data network operations.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

DOI mission critical long distance voice and data communications are primarily provided by WorldCom via the General Services Administration (GSA) Federal Telecommunications System 2001 (FTS2001) contract. Due to WorldCom's Chapter 11 bankruptcy, the DOI reviewed its contingency plans and service alternatives and is closely monitoring WorldCom service status. The DOI is also considering the consolidation of the bureau backbone data communications networks to a single departmentwide Internet Protocol (IP)-based architecture with enhanced network security functionality.

Conversion of DOI's wideband LMR systems to narrowband digital operation is a high priority activity. We continue to

investigate sharing opportunities with the USDA and other cooperators to improve interoperability and reduce costs. We have a multivendor multiyear contract to supply digital narrowband radios and systems in response to the National Telecommunications and Information Administration (NTIA) mandated transition to narrowband LMR operations. This contract, available to all Federal agencies, provides lowercost standardized interoperable digital radios.

Key officials, emergency coordinators, and telecommunications managers throughout the Department have GETS cards for long distance emergency telephone communications. WPS cellular phones have been provided to key officials in Washington, DC. Secure Telephone Units, Third Generation (STU-III) are used to support DOI national security programs, and HF backup radio links are used to augment DOI emergency relocation site communications.

SIGNIFICANT ACCOMPLISHMENTS

- The transition of FTS2000/AT&T services to FTS2001/WorldCom was completed.
- Additional DOI digital narrowband contracts were awarded.
- An LMR system was installed to support DOI continuity of operations requirements.



UNITED STATES DEPARTMENT OF AGRICULTURE (USDA)

NS/EP TELECOMMUNICATIONS MISSION

The USDA has several essential functions requiring NS/EP telecommunications. These functions include providing for the domestic distribution of seed, livestock, poultry feed, fertilizer, and farm equipment, along with inspection of livestock, poultry, and other products to ensure the safety and wholesomeness of food. In addition, the USDA manages the protection and use of national forests, national grasslands, wilderness areas, and other public lands and facilities under USDA jurisdiction. This includes managing wildland fire control activities on these lands in coordination with local authorities, and co-op forestry activities in support of State and local fire protection.

TELECOMMUNICATIONS STAFF ORGANIZATION

USDA's Deputy CIO represents the Agency on the NS/EPC.

Telecommunications Services and Operations, Office of the CIO, provides staff representation for the alternate for the NS/EPC and the COR.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

USDA supports the GETS Program and, in an ongoing effort, ensures all persons in NS/EP leadership positions have GETS personal identification number cards. As an example, GETS cards were issued to all Office of Inspector General (OIG) special agents and Forest Service law enforcement officers and personnel working at the USDA Olympic Command Center and the Winter Olympics and

Special Winter Olympics in Utah. USDA issued GETS cards to critical personnel who were provided WPS VoiceStream handsets. A number of GlobalStar satellite telephones have been distributed to NS/EP personnel.

USDA has begun a departmentwide effort to upgrade all analog STU-III, to digital STE. The need for secure communications is escalating in today's wartime environment. As a result, increased funding is being provided to cover additional secure telephone requirements for HLS, expanded crisis planning operations, continuity of operations relocation sites, and mission areas such as food safety and fire fighting efforts.

USDA obtained TSP authorization for the Natural Resources Conservation Service Montana State Office to support the USDA Forest Service, Gallatin National Forest, Supervisor's Office, and Fire Fighting Dispatch.

The USDA Office of Crisis Planning and Management has begun to utilize the information obtained from the Intelink database as a key component in continuity of operations, continuity of government, and other national security program planning.

USDA also:

- Continues support for the NS/EPC/COR and the National Security Telecommunications Advisory Committee (NSTAC)
- Participates on SHARES-HF Radio Program, Communications Resource Information Sharing Initiative, Federal Wireless Users' Forum, and GETS User Council

- Supports the DOS Diplomatic Telecommunications Service, and
- Participates in Cellular Priority Access Service, Federal Law Enforcement Wireless Users Group, and other working groups as necessary.

NS/EP PARTNERSHIP ACTIVITIES

The USDA and the DOI completed a nationwide agreement for the sharing of common radio frequencies for aircraft operations. This agreement reserves seven radio frequencies used in providing emergency communications, air tactical operations, and flight tracking of government aircraft.

The USDA and the DOS have been collaborating on an agreement to split the very high and ultra high frequency (VHF and UHF) bands between the U.S. and Mexico. One of the benefits of dividing the radio spectrum will be the resolution of radio interference cases along the U.S. and Mexico common border. No existent treaty between the U.S. and Mexico deals with this issue.

Radio interference can endanger the lives of firefighters and law enforcement personnel. USDA has completed an agreement with the Federal Communications Commission (FCC) for the investigation and resolution of domestic and international radio interference. This agreement enables rapid identification and resolution of harmful cases of radio interference nationwide.



DEPARTMENT OF COMMERCE (DOC)

NS/EP TELECOMMUNICATIONS MISSION

The Department of Commerce (DOC) promotes job creation, economic growth, sustainable development and improved living standards for all Americans by working in partnership with businesses, universities, communities and workers to:

- Build for the future and promote U.S. competitiveness in the global marketplace by strengthening and safeguarding the Nation's economic infrastructure.
- Keep America competitive with cutting-edge science and technology and an unrivaled information base.
- Provide effective management and stewardship of the Nation's resources and assets to ensure sustainable economic opportunities.

The DOC touches the daily lives of Americans in many ways. For example, the Department makes possible the weather reports heard every morning and facilitates technology that Americans use in the workplace and at home every day. The DOC supports the development, gathering, and transmitting of information essential to competitive business and makes possible the diversity of companies and goods found in America's (and the world's) marketplaces. DOC also supports environmental and economic health for the communities in

which Americans live, and it conducts the constitutionally mandated decennial census, which is the basis of representative democracy.

These missions are ongoing and sustained during national level NS/EP activities in case of emergencies, including stress periods during peacetime; crisis and mobilization activities; periods of disaster recovery; and during wartime crises such as the events of September 11.

TELECOMMUNICATIONS STAFF ORGANIZATION

The DOC manages its telecommunications through the Office of the CIO.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The following current/ongoing DOC activities support NS/EP objectives:

- The DOC is actively involved in HLS initiatives and efforts to enhance preparedness in the post 9/11 environment with the necessary IT equipment, software, and hardware upgrades. Its headquarters in Washington, DC, is implementing a new, state-of-the-art telecommunications network infrastructure upon which a new VOIP application will run. This new telephone system will include an Emergency Broadcast System that can be used in case of a natural or manmade emergency.

- The National Weather Service staffs in Alaska and Hawaii installed Defense Message System (DMS) terminals and the first phase of the connections to the DMS network to allow the transmission of Tsunami alerts to its DOD customers in the Pacific basin. The DOC headquarters has taken initial steps to prepare and implement a DMS network hub to support the communications of emergency message traffic with DOD and other Federal agencies.

- The DOC has initiated plans for wireless network trunking services and continues its plans for implementing a nationwide wireless trunking service for the connection of isolated wireless networks. This will cover wireless network services, such as cellular, LMR, satellite radio and short wave, over a common service to support the contingency requirements of the Government during all emergencies.

The DOC serves as a lead government agency implementing alternative communications technology with an emphasis on the Internet and electronic-commerce, and methods for protecting Government networks. The DOC continues to increase its use of NCS services and programs, especially in light of the tragic 9/11 events.



DEPARTMENT OF HEALTH AND HUMAN SERVICES (DHHS)

SIGNIFICANT ACCOMPLISHMENTS

- During FY2002, the Department of Health and Human Services (DHHS) continued to utilize the SHARES-HF program in its field-deployable HF radio kits that were developed last year. Civil Air Patrol and Military Affiliate Radio System stations are particularly helpful with on-the-air testing.
- SHARES was also utilized to link the DHHS Office of Emergency Preparedness (OEP) with the field command post of the National Disaster Medical System (NDMS) during the Federal response to the flooding caused by tropical storm Allison in the Houston, Texas, area.
- In addition to the OEP/NDMS, several other operating divisions of the DHHS are considering adding HF radio systems to their Continuity of Operations (COOP) plans. Automatic Link Establishment (ALE) technology makes the use of HF radio more practical for offices that do not have access to trained HF radio operators. OEP/NDMS is indebted to the SHARES program for providing the opportunity to gain experience with this valuable mode of communications.
- Amateur radio operators continue to provide invaluable assistance to NDMS Disaster Medical Assistance Teams (DMAT). Many of the communications officers and telecommunications specialists on DMATs learned their communications and electronics skills through their amateur radio experience. During exercises and actual deployments, amateur radio provides a versatile pool of operators, technicians, and radio frequencies that help HHS to serve the American people.



DEPARTMENT OF TRANSPORTATION (DOT)

NS/EP TELECOMMUNICATIONS MISSION

The Mission Statement outlined in the Department of Transportation (DOT) Strategic Plan asserts that the Department will “serve the U.S. by ensuring a safe transportation system that furthers our vital national interests and enhances the quality of life of the American people.” Towards that end, a DOT Strategic Goal for National Security states that the Department will work to “ensure the security of the transportation system for the movement of people and goods, and advance our national security interests in support of the National Security Strategy.” Since the tragic events of September 11, 2001, the entire Department has been engaged in the evaluation and implementation of enhancements to the safety and security of our transportation systems. The recognition of the vital role that telecommunications plays in providing safety and security to the traveling public, has enabled the Department to further enhance its ability to respond to and counteract new threats as they arise.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The Department participates in several ongoing NS/EP telecommunications activities including:

Support of NCS Activities

The Department continues its active participation on the NS/EPC and its related COR, the President’s NSTAC, and actively supports NS/EP activities and Programs.

GETS

The Department has been involved with the NCS GETS program since its inception. GETS cards have been assigned to Regional Emergency Transportation Coordinators and Representatives across the U.S. and overseas for use during natural disasters and other emergency situations and exercises. The Department has also provided GETS usage sponsorship for state and local government transportation system officials, as well as for key private sector transportation officials.

Other NS/EP Programs

DOT continues to participate in the Federal Telecommunications Committee Standards Program, the SHARES-HF Radio Program, the Communications Resource Information Sharing Initiative, and the TSP System Program.

In the aftermath of the September 11, 2001, terrorist attacks, the Department initiated plans to enhance its existing emergency and disaster telecommunications and data gathering capabilities by consolidating these functions into a new Transportation Information Operations Center (TIOC) facility. Under the management of the Department’s Research and Special Programs Administration (RSPA), the TIOC is being designed to serve as a command center that will provide the capability to: monitor incoming information and breaking news to maintain situational awareness of events affecting the U.S. transportation infrastructure, its systems, and assets; track significant incidents, provide information to the Office of the Secretary and other DOT organizations, Federal Agencies, State and local governments, etc.; and, serve as an operations center for those DOT Operating Administrations

without standalone operations centers. The TIOC will expand DOT’s emergency and situational command capabilities to full 24/7 operation.

National Distress and Response System Modernization Project

The National Distress and Response System Modernization Project (NDRSMP) will be a wireless communications system that provides connectivity between USCG mobile (boats) and portable (handheld) assets and the shore radio net centered at the Group Communications Center (GCC) in the VHF and UHF radio frequency bands. It is designed using the Association of Public Safety Communications Officials’ Public Safety Wireless Network Working Group standards and provides encrypted communications capability. In addition, the NDRSMP will provide the GCC an intercom type feature to contact local NDRSMP equipped shore units. The NDRSMP network will be independent of the commercial phone/cellular service; however, the land connections from the GCC to the remote transmitters are over telecom landlines (data circuits). How the NDRSMP equipment and capabilities are incorporated into emergency response plans is an element of the operational doctrine, developed during Initial Operational Capability deployment and refined during the system operational test and evaluation. NDRSMP implementation is scheduled to begin in FY 2003 with project completion expected in FY 2006.



DEPARTMENT OF TRANSPORTATION (DOT)

continued

SIGNIFICANT ACCOMPLISHMENTS

- The Federal Aviation Administration (FAA) provided significant NS/EP telecommunications support this past year in four functional areas: FAA-to-North American Aerospace Defense (NORAD) Hotlines, Air/Ground Voice Connectivity, Radar Data Distribution, and Aircraft Movement Data.
- The NORAD Hotlines (SCRAMBLE and Sector Operations Control Centers [SOCC]) and were implemented to coordinate FAA activities with Continental U.S. (CONUS) NORAD Region (CONR) Command Center/Air Defense Sectors (ADS).
- Twenty SCRAMBLE Hotline circuits were implemented within two months after September 11, between FAA's Air Route Traffic Control Centers to DOD's ADS/ SOCCs to announce when intercept aircraft are scrambled.
- Twenty-eight SOCC Hotline circuits were installed between DOD's SOCCs to allow the FAA to notify ADSs of any emergencies and for the SOCCs to do the same to FAA.
- The FAA provided NORAD/CONR access to FAA's tactical Air/Ground Voice frequencies. The first phase, 40 circuits, was implemented in October 2001. The second phase will include 73 FAA sites.
- The FAA provided DOD with surveillance data from 70 of the FAA's long-range radars. This was implemented between October and November 2001. An additional 37 Airport Surveillance Radars (ASRs) have been identified to provide further data support. In response to these requirements, the FAA supported the design and implementation of FAA's Bandwidth Manager Network and DOD's Air Combat Command Enterprise Network Gateways.
- The FAA assessed and engineered the distribution of Defense visual flight rules, flight plans, instrument flight rules, and flight movement data to six DOD sites and to the U.S. Customs Service Air and Marine Interdiction Coordination Center.
- In the aftermath of the September terrorist attacks, the U.S. Coast Guard (USCG) identified 20 top tier strategic ports critical to providing HLS. Protection of these ports requires access to classified information, the capability to send and receive critical intelligence and operational planning information to DOD assets, USCG units, and other Federal Agencies. To ensure this capability and interoperability, DOT is providing these Captains of the Port (COTP) with access to the SIPRNET. Connectivity to these initial ports is considered Phase I of the effort to meet this new requirement. Resource and planning proposals have been submitted to expand this service to the remaining COTPs in FY 2003.
- The USCG is currently upgrading most of its HF radio system transmitters and receivers. With this upgrade, the USCG will be establishing ALE networks to improve tactical HF communications reliability and interagency interoperability.



DEPARTMENT OF ENERGY (DOE)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Department of Energy Corporate Network

The Department of Energy Corporate Network (DOENet) is a centrally managed wide area network (WAN) designed to carry critical business sensitive data departmentwide. DOENet currently provides connectivity to 40 sites, each adhering to a uniform connection policy to ensure a minimum level of security. DOENet provides the Department with a private, secure network backbone for the exchange of data between DOE sites using Asynchronous Transfer Mode technology. Connectivity is established at a minimum of 1.544 Mbps with routers to enable simultaneous voice, video, and data services. Centralized management of DOENet provides higher reliability, improved troubleshooting capabilities, greater operational efficiencies, increased accountability, and is essential to maintaining security.

Idaho National Engineering and Environmental Laboratory

Idaho National Engineering and Environmental Laboratory (INEEL) has obtained approval for a connection with the DOD on its SIRNET. This capability will enhance national security safeguards and improve emergency preparedness. The access circuit capability has been installed, and work is progressing in the required in-house extension to this communications capability. The INEEL's innovative approach to transition from

wideband to a narrowband trunked radio system spans several years. Most implementation activities will occur in FY 2002, including the installation of the repeater infrastructure and consoles, purchase of 70 percent of the new radios, and operational testing. The paging system encompasses a geographical area approximately 100 miles in diameter, with coverage extending to locations key to operations and emergency preparedness. Other telecommunications processes and technology activities include the upgrade to INEEL's site-wide telecommunications backbone infrastructure to increase capability; a weather display program that wirelessly collects weather from regional remote stations, allowing for display of current wind speed, wind direction, temperature, and predictive modeling capabilities; and LMRs, both trunked and conventional, with radio console interfaces.

Nevada Operations Office

The Nevada Operations Office has completed the installation and operational configuration of a Reverse 911 dial-back system for emergency coordination at the Nevada Test Site. Nevada is installing new fiber optics cabling and electronics to the Remote Sensing Laboratory at Nellis Air Force Base, which will bring diverse routing, expanded bandwidth, and reliability to the Emergency Response personnel programs. Nevada has initiated a program with its contractor (Bechtel Nevada) to identify critical facilities for telecommunications/computing and to develop operations and maintenance plans for commercial and emergency electrical power support. Nevada is also continuing to install the interconnectivity of the Emergency Communications

Network to the Emergency Operations Center. This involves a new firewall for Internet connection protection.

Oak Ridge Operations Office

The Oak Ridge office continues plans for implementing a wide area radio system to resolve known safety, emergency preparedness, and mutual aid issues. The new trunked-capable narrowband UHF mobile radio system will replace the existing analog, wideband VHF mobile radio system, and provide a central Oak Ridge infrastructure with Oak Ridge-wide connectivity. Oak Ridge continued implementing PKI to support encrypted network traffic. In addition, Oak Ridge continues to support the National Weather Service as a retransmission site for the Emergency Manager's Weather Information Network.

Richland Operations Office, Hanford Site

The Richland Operations Office, Hanford Site Narrowband Radio Upgrade Project is under way and on schedule. The system functional requirements have been developed, the conceptual system design has been produced and approved, and the request for procurement was released for competitive bid. Completion of the award is scheduled for August 15, 2002. The system is scheduled to begin operations by the end of FY 2004. The first phase of this project replaces the aging VHF wideband safeguards and security radio systems with a narrowband trunked radio system capable of digital encryption. The new system allows dynamic communication capabilities for site emergency functions with automated interfaces to Federal, regional, and local safety agencies.



DEPARTMENT OF VETERANS AFFAIRS (VA)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Federal Technology Service 2001 Voice Data and Video Network

Department of Veterans Affairs' (VA) FTS2001 network is primarily provided by Sprint with a few exceptions where WorldCom is the provider.

VA Wide Area Networking

The VA is engaged in a multiphase upgrade of its core network. During the first phase, Sprint, the Federal Technology Service (FTS) vendor supplying VA circuits, will become responsible for managing, monitoring, and maintaining the existing network. The second phase is optimization. Sprint will use the information gleaned in phase one to replace unreliable equipment, simplify network architecture and routing strategies, and improve circuit route diversity. The third phase realizes the goal of relieving VA of designing network architecture, provisioning circuits, detecting hardware incidents, and performing a host of other technical tasks. VA will instead define its business needs and articulate them in the form of Service Level Agreements (SLA). These SLAs will state the performance expected of the network without concern for the vendor strategy chosen to provide the solution.

VA Nationwide Teleconferencing System

The VA Nationwide Teleconferencing System (VANTS) provides audio and video teleconferencing service to the entire VA. VANTS services are primarily used for business meetings, program planning sessions, distance learning, interviews and hearings. VANTS customers include VA employees, emergency personnel, state officials, hospitals, universities and other Government agencies, such as DOD.

The video teleconferencing function of VANTS consists of two multipoint conferencing unit bridges capable of providing multipoint videoconferences at baud rates from 112 Kbps up to 768 Kbps. Sixty-four ports are available to support the most commonly used bandwidth of 384 Kbps. The video bridging services run over Integrated Services Digital Network and allow connectivity from various networks throughout VA. The only costs associated with the use of this service are the long distance charges incurred when dialing a video teleconference. These costs vary in accord with the user's video network configuration and the long distance provider. This technology allows VA employees to conduct "face-to-face" meetings without the time and expense of travel.

The audio function of VANTS currently has 768 audio ports for voice teleconferencing. Participants are provided a toll-free number and an access code for easy access from any telephone within CONUS.

Offshore Satellite Service

The Office of Telecommunications coordinates offshore Satellite Telephone Service via the International Maritime Satellite Organization (INMARSAT) to provide emergency voice and data telecommunications service to VA facilities operating in U.S. territories and possessions. Multiple portable terminal platforms are provided to ensure survival of communications facilities under the most severe natural phenomena. The INMARSAT system has been proven successful in emergency and recovery operations resulting from several hurricane events in recent years.

VA Southern California Emergency Communications System

The VA's Southern California Emergency Communications System UHF radio system was integrated into the Los

Angeles Federal Government Wireless Trunking Network. Conversion from the existing analog, shared frequency radio system to the wide-area, digital trunking system provided service to a widely expanded area with a vastly increased capacity for voice, secure voice, and data communications. The Federal Trunking System is linked to all Federal and civil emergency service and law enforcement providers in the Los Angeles Basin.

New OIG Network

The VA Radio Frequency Management Office, working with the IG, has completed implementation of a nationwide, narrowband fixed/mobile radio network. The new VHF network integrates the investigative arm of the OIG with Federal and civilian law enforcement services nationwide, and provides unique narrowband radio frequencies for six VA regions. The new radio system provides the highest degree of security in communications available today for IG field operations.

Frequency Management Automation

As radios proliferate in the VA workplace, and the radio frequency spectrum becomes nearly saturated in every Federal frequency band, engineering a new radio frequency for a hospital or cemetery has become a complex task.

To simplify the process, the radio Frequency Management Office acquired a new frequency management tool in the form of a Windows NT compliant software package called Spectrum XXI (SXXI). The new tool allows VA technicians to compartmentalize the gigantic Federal Government Master File of Radio Frequency authorizations into VA regions, which reduces the number of records involved in a search for a new frequency. A search that once took 6 or more hours can be completed in about 20 minutes, allowing two to three technicians to do the work that formerly required six to eight highly skilled specialists.



CENTRAL INTELLIGENCE AGENCY (CIA)

NS/EP TELECOMMUNICATIONS MISSION

The NS/EP telecommunications mission of the Central Intelligence Agency (CIA) is to ensure the secure flow of all-source foreign intelligence information to the President and other selected national policy makers. To this end, the CIA provides secure, rapid, and reliable round-the-clock telecommunications and information services that are:

- Modern, efficient, and interoperable to support intelligence collection and distribution requirements

- High volume and timely for open-source collection
- Quick-reacting in support of crises and special operational requirements wherever needed.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Information Services Infrastructure operates, manages, and maintains the CIA's messaging, telecommunications, and information services capabilities. The agency also provides telecommunications support to other U.S. Government departments, agencies, and the military services as required to support intelligence requirements.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The following CIA activities support NS/EP objectives:

- Active participation in the NCS activities of the NS/EPC/COR
- Continued support of the GETS, the Federal Telecommunications Standards Committee, the TSP System, and the SHARES-HF.

SIGNIFICANT ACCOMPLISHMENTS

- Continued to develop a cadre of professional personnel prepared to meet operation, technical, and system management requirements of modern telecommunications and automated information systems.
- Provided enhanced telecommunications services between the CIA and the U.S. military services.
- Continued support to DMS objectives and architecture.



FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

NS/EP TELECOMMUNICATIONS MISSION

The Federal Emergency Management Agency's (FEMA) mission is to reduce the loss of life and property and protect the U.S. institutions from all hazards through a comprehensive, risk-based, emergency management program of mitigation, preparedness, response and recovery. In addition to FEMA's long-standing goals of protecting human lives, reducing human suffering, and preventing the loss of property, the Agency has added two more goals to its draft 2002-2008 strategic plan. The additional goals are to prepare the Nation to address the consequences of terrorism and serve as the Nation's portal for emergency management information and expertise.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

FEMA continues to develop and coordinate its all-hazards disaster programs among Federal departments and agencies, State and local governments,

and other public and private sector organizations while responding to Presidential disaster declarations. Subsequent to the terrorist attacks of September 11, the Agency was tested in unprecedented ways as it focused on issues of national preparedness and HLS. The Agency coordinated its activities with the newly formed Office of HLS, and is actively directing its approach to disasters toward HLS issues. FEMA has been directed to help communities face the threat of terrorism, and its Office of National Preparedness was given the responsibility for helping to ensure that the Nation's first responders are trained and equipped to deal with weapons of mass destruction (WMD). To benefit from their experience and to increase the preparedness of first responders, FEMA is endeavoring to establish working relationships with State and local public safety and first responder communications associations.

FEMA now manages two of the three "Level Three" e-Government initiatives requiring direct involvement of the President's Management Council. The first, the Disaster Management e-Government Initiative (Disasterhelp.gov), focuses on

establishing a customer-centric portal for delivering integrated Federal, State, local, tribal government, and nongovernment organizations; all-hazards information and services. The initial focus is on providing information and services related to all aspects of disaster management, with emphasis on the needs of first responders. The Web site consists of existing information and services with links to other sites. Later phases will incorporate delivery of integrated, cross-agency processes and services, resulting in a full-blown portal with its own search engine.

On May 31, 2002, FEMA became the managing partner for a second initiative, the interagency Wireless Public SAFECOM. All Federal Government programs and resources currently devoted to public safety wireless communications interoperability are to be consolidated under this initiative. The objective is to eliminate duplication, improve business processes, and ensure the successful delivery of interoperable wireless communications solutions to customers at the Federal, State and local levels. SAFECOM's scope encompasses all Federal departments with public safety and HLS missions.

SIGNIFICANT ACCOMPLISHMENTS

- Disasterhelp.gov became available to internal partners in September 2002.
- When FY 2002 began, FEMA was supporting 11 declared disasters. Since then, FEMA has responded to over 34 additional Presidentially declared disasters. The support included the deployment of Disaster Response Teams to install telecommunication resources at Disaster Field Offices (DFO); processing of 78 TSP requests for provisioning new data and/or voice T-1s; the reprocessing/recycling of used equipment and shipping of 18,000 pieces of IT equipment needed for DFO operations; and the processing billing of approximately \$12 million for new IT services in support of disaster operations.



THE JOINT STAFF (JS)

NS/EP TELECOMMUNICATIONS MISSION

The Director for Command, Control, Communications and Computer (C4) Systems (J6), provides advice and recommendations on C4 matters to the Chairman of the Joint Chiefs of Staff (CJCS) and to the JCS. The J6 develops policy and plans, monitors programs of joint C4 systems, and ensures adequate C4 support to the NCS, commanders in chief, and warfighters for joint and combined military operations. The J6 leads the C4 community, conceptualizes

future C4 system architectures, and provides direction to improve joint C4 systems. The J6 oversees C4 support for the National Military Command System.

TELECOMMUNICATIONS STAFF ORGANIZATION

The J6 Directorate is led by the Director and Vice Director. The Director chairs the Military Communications-Electronics Board for the Secretary of Defense. The Director and Vice Director are general/flag officers from the military departments. The J6 Directorate includes a functionally aligned Division, a Programs and Budget section, and a Director’s Action Group.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

(Refer to DOD Section)

PENDING ISSUES

(Refer to DOD Section)

SIGNIFICANT ACCOMPLISHMENTS

(Refer to DOD Section)



GENERAL SERVICES ADMINISTRATION (GSA)

NS/EP TELECOMMUNICATIONS MISSION

The GSA FTS NS/EP mission is to ensure that federally owned or managed domestic communications facilities and services meet the NS/EP requirements of the Federal Government.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

- The GSA FTS provides a full time detailee to support the National Crisis Coordinating Center at the NCS. The GSA also ensures that an NCS Regional Manager (NCSRM)/GSA Regional Emergency Communications Planner (RECP) and Federal Emergency Communications Coordinator are identified for each of the 10 standard Federal regions and the National Capital Region. These personnel assist the FEMA, the Office of Science and Technology Policy, and the NCS during disasters and national security emergencies.
- The GSA FTS provides a full range of network services and IT solutions that meet the current and future needs of the Federal Government with globally positioned NS/EP capabilities, resources, services, and solutions. NS/EP services are also available to tribal governments, as well as State and local governments, with the sponsorship of a Federal Government department or agency.
- GSA FTS has augmented the FTS2001 contracts with WorldCom and Sprint by adding services provided by AT&T and Qwest via the FTS2001/Metropolitan Area

Acquisition (MAA) Crossover program. The addition of these two industry partners provided government agencies with increased diversity and security in the management of their communications networks. FTS2001 and Crossover bring advanced, state-of-the-art, commercial-grade services to Government locations around the world. Customers at 165 Cabinet level departments and independent agencies benefit from FTS service.

- The GSA FTS continuously monitors the security, reliability, and survivability of the FTS2001 networks provided by its industry partners. GSA requires a specific level of service to be maintained during periods of severe overload on the Public Switched Network. The FTS2001 and Crossover networks are required to maintain the most advanced security features available. The GSA FTS industry partners work with the Government to reassess the severity of new or perceived threats and, when necessary, take countermeasures to assure the specified network availability in accordance with the network security and reliability plans.
- Multi-Tiered Security Profiles (MTSP) is an initiative of the FTS designed to provide enhanced network service offerings by integrating various security layers into the current portfolio of contracts. MTSP projects that contract modifications will be in place and begin offering the first tiers of MTSP by the end of 2002.
- The FTS provides contract vehicles for worldwide telecommunications services, international direct

distance dialing, wireless voice and data, satellite services, Internet access, technical services support, information security services, and services necessary to support CIP and the Government Information Security Reform Act (GISRA). Examples are the GSA FTS Safeguard Program, a tool kit of security products and services; and the Access Certificates for Electronic Services contracts that facilitate secure online public access to Government information and services.

- Managed Security Services (MSS) via the Safeguard Program promote the development and deployment of capabilities that provide Federal agencies and departments the ability to proactively protect their information systems and resources. MSS allows agencies to select services such as intrusion detection, audit trail analysis, incident reporting, and several other network management capabilities aimed at improving the overall security profile and protection strategies for Federal IT.
- GSA's Federal Computer Incident Response Center (FedCIRC) provides a trusted focal point for computer security incident reporting, offering assistance with incident prevention and response to the Federal Government. FedCIRC provides a variety of services and programs, at no cost to agencies, enabling Federal agencies to work together to identify and handle security incidents, share related information, and solve common security problems.
- FedCIRC collaborates with the National Infrastructure Protection Center, the National Security



GENERAL SERVICES ADMINISTRATION (GSA)

continued

Incident Response Center, the DOD

Computer Emergency Response Team (CERT), the Carnegie Mellon CERT Coordination Center, and several IT industry partners. The purpose of these collaborations is to develop and ensure effective defenses against malicious program activities and to provide containment and recovery assistance to Government components that have been victims of computer security related events, such as an unauthorized intrusion, computer virus, and other occurrences posing a threat to IT resources supporting critical mission functions.

- The GSA FTS Safeguard Program provides products and services to assist agencies in meeting their requirements under the GISRA, annual IG security evaluations, agency reporting to the OMB, and annual OMB reports to Congress. The Safeguard Program allows an agency to design, implement, maintain, and modify its security

architecture to conform to its particular requirements.

- The FTS Next Generation Strategy (NGS) is to plan 5 to 10 years out for the FTS Next Generation of IT/telecommunications solutions based on a common vision of the right relationships, products, and processes that will ensure a successful future of continued services to federal agencies. The first phase of the NGS will be the network services follow-on for the expiring FTS2001, MAA, and Niche contracts due in FY 2003.
- The FTS is developing a Web services initiative that seeks to examine the technology and product offerings that could be leveraged to complement existing Federal e-Government initiatives. The goals of this initiative are to identify the service providers, ensure the availability of these providers through existing FTS contracts, combine Web Services with other Federal entities to provide total

solutions for client agencies, and develop a "go-to-market" strategy.

- The GSA FTS offers a vast array of services on its constantly updated wireless and satellite services contracts. The service is ideal for agencies that need to broadcast on an occasional basis and reach many sites. The Centers for Medicare and Medicaid Services (CMS) have made innovative use of DirecTV services to support their distance learning network. The CMS network will support approximately 75 continental U.S. locations and provide the ability to broadcast high-quality video programming at low cost. The FTS is also working with the NCS to establish WPS for emergency response and HLS.
- The FTS supports the NCS and the NSTAC through participation in fact-finding and analysis meetings, providing a Government perspective to industry studies used to develop NS/EP recommendations to the President.

SIGNIFICANT ACCOMPLISHMENTS

- GSA has provided support to FEMA in terms of the Federal Response Plan (FRP) and responded to the emergency requirements of several Federal agencies this FY. FTS Emergency Communications Coordinators have supported Emergency Support Function (ESF)-7 (Resource Support) and ESF-2 (Telecommunications) of the FRP, from the ongoing major floods and fires in the western and south central U.S. to the typhoons in Guam.
- FTS is providing the voice telecommunications requirements for the Transportation Security Administration installations with WorldCom and Sprint to 597 commercial airports around the U.S. This involves installing 25,000-30,000 voice lines, telephones, and wiring. Also included is access to CNN and local television stations. In addition to the voice communications requirement, FTS is providing wireless services including cellular and paging services.
- The FTS supported the Bureau of Diplomatic Security, Countermeasures Program Division, Technical Surveillance Countermeasures Branch (DS/CMP/TSC) and the DOS Computer Security Program. Major program tasks included supporting and conducting special TSC Mitigation (TSCM) investigations and inspections, evaluation of new technologies and devices, specialized TSCM training, the procurement, design and enhancement of TSCM equipment, independent security verification and validation, and internal/external security vulnerability assessment. FTS also provided TSCM equipment inventory logistics support to approximately 55 overseas Engineering Security Centers and Offices, and five domestic branches of the DS.



GENERAL SERVICES ADMINISTRATION (GSA)

continued

- The FTS supported the USDA Cyber Security Program Office in the development of its Information Survivability Program. Specifically, FTS supported the development of disaster recovery and business resumption plans for mission-critical USDA programs and systems that support the Information Survivability Program. The work will benefit all USDA agencies with attention paid to USDA's most critical and sensitive systems.
- The FTS supported the DOT RSPA in improving its IT Security Program. RSPA required professional security services to assist, advise, and participate in the improvement of all aspects of the current security program. Specifically, FTS assisted RSPA in developing and implementing a DOT security plan that identifies roles for an information system security office, system owners, designated approval authorities, system administrators/system security administrators, users, the incident response capability to be activated, and the metrics that will be used to measure program performance.
- The FTS supported the Equal Employment Opportunity Commission (EEOC) emergency planning contingency efforts. Specifically, support involved contingency planning and disaster recovery for a computer and telecommunication facility. FTS conducted a risk assessment of the computer facility, documented the findings and made recommendations, including an off-site backup computer facility that could be utilized in the event of an emergency. In addition, FTS supported the development of an IT contingency plan for the EEOC headquarters computer room, the local area network (LAN)/WAN, equipment, and facilities.
- FedCIRC's initiative for the Patch Authentication and Dissemination Capability will provide Federal agencies and departments a no-cost method of receiving notification of hardware and software vulnerabilities as they become known, pending security fixes that mitigate the vulnerabilities, and notification when vendor patches have been authenticated and validated.
- The FedCIRC Operations Assessment (Process Analysis) is being conducted to analyze FedCIRC's processes and relationships with Federal civilian agencies, academia, and private industry. This assessment provides assurance that FedCIRC's coordination, reporting analysis and incident response processes provide a cost effective, value-added service to the Government customer. Additionally, FedCIRC offered a Web based customer communications survey to solicit customer feedback concerning the quality and types of services FedCIRC currently provides.
- A Request for Proposal for the FedCIRC Web Portal will be released in late July. The FedCIRC Web portal will serve as a gateway for IT leaders and security professionals to improve cross-governmental information sharing and collaboration. The Portal will deliver a secure method for on-the-spot incident reporting; special access to FedCIRC's Web-enabled security patch management services; access to documentation and training for establishing and augmenting Agency incident response capabilities; as well as other items of interest for secure computing.
- As of June 30, 2002, FedCIRC had responded to 5,531 incidents. These included 52 Web site defacements and 53 incidents in which intruders gained control of a victim's computer. Additionally, FedCIRC has issued 30 Advisories, 16 Informational Notices, and 85 Special Communications.
- The GSA FTS New England Region has initiated the deployment of smart card technology in two of its GSA managed Federal office buildings in Boston and will continue the plan for the entire region next FY. Approximately all of the 280 GSA associates in the New England Region will be issued smart cards by the end of FY 2002. Smart Cards will be interoperable with all other GSA Facilities and any other facilities employing Government Smart Card-Interoperability Standards.
- The FTS New England Region will host a seminar in September for the FEMA Regional Interagency Steering Committee in coordination with the NCS. The Great Lakes Region will host a similar seminar in October. These seminars will focus on the responsibilities of the Emergency Response Team (ERT) with regard to emergency communications employment during a disaster and telecommunications restoration in the aftermath.
- Following the events of September 11, 2001, the GSA-FTS Southeast Region RECP/ NCSRM was invited by the FEMA Federal Coordinating Official to help develop the new annex to the National FEMA ERT-National WMD Plan. GSA's contribution to this effort involved rewriting the communications section of the annex and explaining how the NCS would interface with FEMA and the other Federal agencies following this type of incident in the future.



GENERAL SERVICES ADMINISTRATION (GSA)

continued

- GSA-FTS Mid-Atlantic Region and Southeast Region have ordered TSP on its Private Branch Exchange (PBX) trunking in those Federal buildings where FTS provides service via a PBX. This ensures priority restoration of GSA trunk circuits in the event of a catastrophic outage. Other GSA-FTS regions will be researching and implementing this important customer service program.
- Since 1999, FTS has awarded 44 MAA contracts in 25 metropolitan areas across the Nation. Two-thirds of the Federal workforce are now within reach of an MAA, with attractive prices and state-of-the-art service offerings.
- When Winstar Communications faced liquidation before the Bankruptcy Court of Delaware, GSA's FTS teamed with DOJ and the FCC to ensure that the Government's interests were fully represented. During this process, FTS updated its contingency plans to enable quick response should bankruptcy court decisions become unfavorable to the interests of our customers. Fortunately, Winstar was purchased by IDT and the crisis was averted.
- GSA has initiated a project to encompass the three GSA business lines — FTS, Public Buildings Service (PBS), and Federal Supply Service—chaired by the Deputy Regional Administrator, Mid-Atlantic Region in Philadelphia. This team will provide for the coordinated delivery of the full range of services available from GSA.
- PBS and FTS have partnered in suggesting telecommunications service access approaches to a House Appropriations Subcommittee that is working to ensure continuity of telecommunications services for Government agencies with critical needs.
- FTS has reviewed and analyzed commercial and contract rates for FTS service categories, as provided by the Price Management Mechanism specification of the FTS2001 contract, to determine if price reductions were warranted.
- GSA FTS has enhanced their FTS2001 contracts with WorldCom and Sprint to provide increased physical and network security. Through FTS2001 contract modifications, Federal agencies can now obtain managed firewall services, managed hosting services, and Internet collocation services.
- FTS has lowered its management fee for the FTS2001 contracts from eight percent to seven percent. This price reduction will allow agencies to better manage their telecommunications budgets and redirect resources towards more pressing NS/EP requirements.
- The FTS provides vendors and agencies access to all their services, including disaster support, contingency planning, and continuity of operations services through the GSA home page (<http://www.gsa.gov>).



NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA)

NS/EP TELECOMMUNICATIONS MISSION

The National Aeronautics and Space Administration (NASA) Administrator shall (pursuant to E.O. 12656) coordinate with the Secretary of Defense to prepare for use, maintenance, and development of technologically advanced aerospace and aeronautics-related systems, equipment, and methodologies applicable to national security emergencies.

TELECOMMUNICATIONS STAFF ORGANIZATION

NASA's Associate Administrator for the Office of Space Flight has programmatic responsibility for representing the organization, on behalf of the Administrator, in the NCS process. The Associate Administrator for Space Flight assigned the Assistant Associate Administrator for Space Communications as NASA's NS/EPC representative.

NASA's George C. Marshall Space Flight Center, located in Huntsville, AL, maintains responsibility for the operation of NASA's telecommunications and data networking infrastructure, known as the NASA Integrated Services Network (NISN).

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

NASA continues to support the NCS in achieving its assigned missions and the successful accomplishment of national-level programs approved by the White House. This includes TSP, Communications Resources Information Sharing, Federal Telecommunications Standards Program, Cellular Priority Access Service, Enhanced Satellite Capability, Emergency Response Link, and the National Telecommunications Management Structure.

NASA also continues to actively participate in the SHARES-HF, GETS, Interagency Committee on Search and Rescue, the Federal Wireless Users Forum, and the NCS Technology and Standards Accomplishments.

NASA/EP TELECOMMUNICATIONS ASSETS

- The NISN supports both space flight critical communication services and day-to-day administrative and scientific applications within the Agency, its contractor and research partners, and International Space Partners.

- NASA Tracking and Data Relay Satellite System is a constellation of geo-stationary satellites providing almost uninterrupted communications with NASA's Earth-orbiting spacecraft and other supported customer satellites.
- NASA Deep Space Network supports deep space interplanetary, high-Earth orbiting spacecraft, and radio science missions.
- NASA Ground Network (GN) supports low-Earth orbiting space flight missions. NASA is currently studying the commercialization of the GN facilities.
- NASA Research & Education Network is NASA's component to the Next Generation Internet initiative. It operates as a test bed for developing Internet technologies, applications, and networking tools.

SIGNIFICANT ACCOMPLISHMENTS

- Continued to meet established service performance levels despite growing usage and customer requirements.
- Compressed mission voice service provisioning to a lower data rate.
- Implemented electronic scheduling and "meet-me" services for voice teleconferencing.
- Implemented intrusion detection and incident response systems for data services.
- Implemented the NASA secure network to accommodate secure voice and data capability between NASA centers.
- Implemented several network and service upgrades to support NASA employees in Russia.
- Implemented an automated subscription and distribution system for network activity and outage notification.



NUCLEAR REGULATORY COMMISSION (NRC)

**NS/EP
TELECOMMUNICATIONS
MISSION**

The Nuclear Regulatory Commission (NRC) is responsible for ensuring adequate protection of public health and safety, common defense and security, and the environment with respect to the use of nuclear materials for civilian purposes in the U.S. Activities licensed and regulated by the Commission include commercial nuclear power reactors; nonpower research, test, and training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste.

The Commission’s NS/EP telecommunications provide for highly reliable connectivity between the NRC Operations Center, operating nuclear power plant control rooms, emergency operations facilities, and regional incident response centers. This connectivity ensures immediate notification to the NRC Operations Center of unusual occurrences and provides relevant information during accidents/events at NRC licensed facilities.

**CURRENT/ONGOING NS/EP
TELECOMMUNICATIONS
ACTIVITIES**
The NRC Emergency Telecommunications System (ETS), which provides NS/EP communications from nuclear power plants and major fuel cycle

facilities, consists of FTS 2001 Direct Access Lines at most locations. At 23 sites, ETS is provided using the utilities’ corporate communications systems. GETS has been highly recommended as a means of enhancing access to long distance service. TSP coverage is assigned to at least one circuit at each FTS2001 served ETS site. The NRC is working to add secure teleconferencing capability to the ETS.

SIGNIFICANT ACCOMPLISHMENTS

- NRC encouraged licensee use of GETS as a part of contingency plans.
- GETS use has been promoted as a means of improving emergency telecommunications at nuclear power plant sites.
- TSP coverage has been employed on primary FTS2001 ETS circuits.
- GETS access numbers were used during the NRC response to the September 11 attacks.



NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

NS/EP TELECOMMUNICATIONS MISSION

The NTIA NS/EP mission as tasked under E.O. 12046, 12472, and 12656 includes serving as the executive branch telecommunications policy adviser to the President, manager of Federal Government uses of the radio frequency electromagnetic spectrum under all conditions, and as a member of the Joint Telecommunications Resource Board. NTIA advises and assists the President in administering a system of radio spectrum priorities for spectrum-dependent telecommunications resources of the Federal Government that support NS/EP functions.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The NTIA/Office of Spectrum Management (OSM) continues to plan and implement, using a phased approach, a series of Federal spectrum management system improvements relative to a total electronic transfer capability and the use of Federal spectrum management data and information. It also continues to develop, field, and maintain several management automation tools for use by Federal spectrum managers to more effectively plan, coordinate, and control the use of the radio frequency electromagnetic spectrum during NS/EP and normal conditions. Examples of these activities include:

- Partnered with the DOD's Joint Spectrum Center to develop and field:

- ▶ SXXI Versions 4.0 (estimated release date of December 2002) and 3.0 (released November 2001), the follow-on spectrum management software to Versions 3.0 and 2.0 respectively, for use by all Federal spectrum managers

- ▶ For evaluation and testing, the Beta-test version of an icon-based, graphical user interface supported by sophisticated logic that will serve as the method Federal agencies use to develop and submit spectrum certification requests to NTIA

- ▶ The Beta-test and initial operating capability versions of the Statistical Database Viewer to display in several ways various spectrum information, including allocation tables and associated spectrum-use statistics and

- ▶ For NTIA/OSM staff evaluation and testing, the text-based prototype, Table of Allocations Manager.

- Implemented the architecture for alternative site processing of Federal spectrum management data, communications, and operations for NTIA essential personnel.
- Completed a prototype Web-based server capability for use by several agencies of the Federal spectrum management community to access and exchange electronic (digital) copies of official, unclassified, the Inter-department Radio Advisory Committee (IRAC) documentation.

- Completed and distributed the new Version 6.01 of the Microcomputer Spectrum Analysis Models for Windows for use by all Federal spectrum managers and others.
- Revised the NTIA Federal Spectrum Management System/IT Improvements Plan to include planned outcomes, improvement goals, and an estimated completion date for each identified improvement.

In addition, the NTIA/OSM-

- Participated in national emergency management communications activities and endeavors.
- Participated in GETS User Council activities and endeavors and provided GETS user authorizations to new NTIA emergency essential personnel.
- Participated in various activities and endeavors of NSTAC.
- Participated in activities and endeavors of the NS/EPC and its related COR.
- Participated in the NCS SHARES-HF Coordination Network Interoperability Working Group activities and endeavors.
- Participated in the National Science and Technology Council's CIP Research and Development Interagency Working Group activities.



NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA) *continued*

SIGNIFICANT ACCOMPLISHMENTS

- Conducted over 200 meetings of the IRAC and its subcommittees and ad hoc groups.
- Processed over 75,000 frequency assignment actions submitted by Federal agencies for new frequency assignments or revisions of existing assignments.
- Represented the U.S. Government on many spectrum policy matters at various International Telecommunication Union meetings and other international and regional meetings.
- Served as the Lead Agency for the Information and Communications (I&C) Sector of the Nation's critical infrastructures; as such, chaired the I&C Sector Working Group and its subcommittees to promote information sharing and coordinated action to mitigate CIP risks and vulnerabilities in all levels of the I&C Sector.



NATIONAL SECURITY AGENCY (NSA)

NS/EP TELECOMMUNICATIONS MISSION

The NSA has an operational mission to support the critical intelligence needs of the DOD and national security community, and to provide the technical support necessary to develop and maintain the security and protection of NS/EP telecommunications.

IT AND INFORMATION ASSURANCE ORGANIZATIONS

Within NSA, two organizations share responsibility in supporting NS/EP-related activities. The IT Infrastructure Services group is responsible for planning and operating the telecommunications systems and networks linking Agency elements worldwide, and for providing Agency connectivity to other Government services.

The Information Assurance (IA) Directorate is responsible for developing and providing information security (INFOSEC) products and services to enhance the security of telecommunications systems. Both organizations work in close collaboration with military services and defense agencies in support of overall DOD initiatives. In accordance with its National Manager responsibilities under National Security Directive 42, INFOSEC products and services are also applicable across the Government for the protection of classified and sensitive national security information. NSA's customers include a broad range of users of the National Information Infrastructure and the critical infrastructure communities. IA activities include a close working relationship with the National Institute of Standards and Technology (NIST).

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Support to Counter-Terrorism and Operation Enduring Freedom

- NSA continues to develop and make available IA solutions for the U.S. Government to support national and international activities.
- Created the NSA HLS Support Office to incorporate Information Superiority capabilities into America's framework for HLS and infuse an HLS emphasis into NSA's mission and culture.
- Providing IA products and security systems on an emergency basis to protect voice and data communications across the national security community. This support has included installation, training, and cryptographic keying material.
- The NSA Interagency Operations-Security (OPSEC) Support Staff (IOSS) continues, and has had increased requests, to assist in improving the U.S.' OPSEC posture by providing awareness, training, and support to any U.S. Government organization.

DOD PKI

- Continued to lead, in partnership with the DISA, the DOD PKI Program Management Office. Release 3 of the DOD PKI became operational in October, 2001, and included the ability to issue PK certificates on Common Access Cards (CAC). As of July, 2002, over one million DOD employees have received PK certificates including over 700,000 on CACs. In addition,

continued deployment and improvement of the DMS has occurred.

National IA Support

- Continuing to lead the activities of the Committee on National Security Systems for the ASD.
- Leading the support to enable the implementation of the National IA Acquisition Policy (NSTISSP-11). As of July 1, 2002, all U.S. Government Departments and Agencies are required to acquire, for use on national security systems, only those IA or IA enabled products that have been evaluated or validated in accordance with the requirements of NSTISSP-11.
- Strengthening the partnership between NSA and the NIST to grow and maintain the National Information Assurance Partnership's Common Criteria Evaluation and Validation Scheme, and to enable the successful implementation of NSTISSP-11.
- Sponsoring and developing protection profiles for products and systems including firewalls, VPNs, remote access, databases, operating systems, single level web, tokens, intrusion detection systems, PKI, mobile code protection, wireless biometrics and directory services. In 2002, seven new protection profiles were published.

Coalition Interoperability

- Leading the evolution of IA products and IA systems security engineering services to ensure a state-of-the-art means to provide secure coalition communications capabilities.



NATIONAL SECURITY AGENCY (NSA) *continued*

- Established a program office to continue the efforts of the U.S. Joint Forces Command to develop a Content-Based Information Security solution to provide secure bilateral and multi-lateral coalition information exchanges.

Information Assurance Technology Development and RollOut

- Continuing to develop high assurance IA products and technologies to address the needs of U.S. Government.

Wireless

- Developed and delivered an integrated secure voice and data handset solution for Code Division Multiple Access.
- Developed and delivered a secure voice and data module that "clips on" to a commercial tri-mode Global System for Mobile handset.
- Developed and delivered secure Wireless LAN (WLAN) product to provide data security through a commercial 801.11 WLAN.
- Developing a modification to a commercial mobile e-mail device to add DOD PKI capabilities to provide increased assurance for sensitive e-mail.

High Assurance IP

- Created and leading an industry/Government team that is developing a common High Assurance IP Interoperability Standard to develop future IP in-line encryptors.
- Initiated the development of a high assurance, robust Key Management

Infrastructure (KMI). The first Capability Increment for the KMI will provide DOD PKI Release 4.0 and common key management services supporting other traditional IA capabilities.

Crypto-Modernization Initiative

- The Crypto-Modernization Initiative is continuing to gain momentum toward the modernization of the DOD's IA capabilities to replace an aging cryptographic product inventory, meet increased interoperability requirements, keep pace with information technology evolution and achieve the vision of Defense in Depth espoused by the GIG initiative.
- Planning and partnership with each of the Armed Services is continuing to increase as numerous NSA and service specific activities have been initiated.
- NSA IA products and supporting infrastructures, currently in development, have addressed enabling modern cryptography.
- NSA has hosted two industry and Government forums to share issues and concerns.

Support to National Critical Infrastructure Issues

- Provided services including threat, vulnerability, and risk assessments to member organizations that provide security guidance and advice, especially with respect to dependence on the critical infrastructures.
- Provided security guidance for ongoing NCS programs, including Wireless Priority Access Services (WPAS).

National Security Incident Response Center

- The National Security Incident Response Center (NSIRC) provided expert assistance to the national security community regarding computer network defense. This was accomplished through unique, tailored, time-critical and term reporting based on NSIRC's ability to detect, react, warn, and respond to intrusions into U.S. Government cyber networks and to provide all-source threat reporting on Signals Intelligence threats to operations, exercises, information systems and force protection.
- The NSIRC partnered with other NSA offices, organizations within the DOD, the Intelligence Community, other Federal Agencies through the Federal Computer Incident Response Capability, the National Infrastructure Protection Center, the NCS, the Network Security Information Exchange, industry, academia, and others to share information about, and respond to, cyber events.
- The NSIRC Desk Officer, a 24/7 time-sensitive operations desk within the National Security Operations Center, focused on detecting and alerting the national security community partners of cyber events. Among other mechanisms used for sharing information about these events, the NDO was a key player in employing the Cyber Warning Information Network, which is designed to alert national security community partners to cyber activity.



UNITED STATES POSTAL SERVICES (USPS)

NS/EP TELECOMMUNICATIONS MISSION

The U.S. Postal Service (USPS) delivers more than half of the world's mail. In support of that effort, we maintain one of the largest computing infrastructures in

the world. Our infrastructure is comprised of more than 547,000 hardware components that support 170,000 users utilizing more than 1,100 business applications in over 14,000 locations—every day. And every day, the IT organization gets the job done—securely, efficiently, and economically.

The USPS has not been assigned any specific NS/EP telecommunications

responsibilities in the event of a national emergency or other declared disaster. Therefore, the USPS designs, engineers and develops telecommunications systems, services, and solutions to support day-to-day organizational, administrative, and operational mission requirements.

SIGNIFICANT ACCOMPLISHMENTS

- During FY 2001, the Postal Service developed the infrastructure plan for a uniform, distributed computing environment within the Postal Service. Named the Advanced Computing Environment (ACE), we anticipate the initiative will save the Postal Service more than \$100 million over 5 years. In FY 2002, the ACE rollout began. Over 2,500 USPS Headquarters employees have been migrated to ACE, and district help desk consolidation has begun.
- ACE deployment will include reducing 270 standard software packages to 60, 85 District help desks to one, 13,000 servers to 1,500 (but with increased capacity), and 11,000 support locations to 540.
- During FY 2002, the Postal Service also deployed Active Directory infrastructure for a single sign-on capability, removed more than 3,700 servers from service—reducing redundancy, maintenance, and management costs and negotiated contracts for help desk consolidation, ACE deployment, and e-mail replacement, saving more than \$10 million.
- As of the end of FY 2002, almost 400 Blackberry wireless communications devices had been deployed to Postal Service executives. This service has proven so popular that several managers are purchasing the devices and services for their staff members who travel extensively to increase their productivity.
- The IT Portfolio groups launched a comprehensive effort to improve systems availability through process management and development of systems availability performance metrics and indicators. This effort resulted in an improvement of systems availability overall to the point that systems were up and running an unprecedented 99.87 percent of the time during FY 2002, surpassing all SLAs requirements.
- During FY 2002, the USPS IT Corporate Information Security Office made significant progress in creating a climate where employees, customers, and partners understand that security brings real business value to our products and services. The USPS had no significant breaches or viruses that could have prevented us from serving our customers or conducting our day-to-day business functions.
- Also during FY 2002, the USPS designed and put into operation the initial elements of a layered defense that includes strengthening firewalls, guarding the network perimeter, implementing initial baseline hardening standards, and enhancing access controls.



UNITED STATES POSTAL SERVICES (USPS)

continued

SIGNIFICANT ACCOMPLISHMENTS

- Supplementing the USPS layered defense initiative are enhanced intrusion detection software, scheduled infrastructure vulnerability assessment tests that include critical and high-risk sites as well as identified vulnerabilities, and scheduled network scans to identify potential risk areas.
- In addition, we established crisis management and incident response teams to identify, contain, and respond to security threats, including the development of COOP procedures and shadow infrastructure to ensure the continuity of essential business functions in the event of a wide range of emergencies or threats.
- The USPS is working with DOD to improve the electronic presentation of mailing addresses, and to promote adherence to domestic and international mailing requirements. The project involves development of postal address information in an XML format that will make it easier to generate data and communicate internationally via the Web.
- This past year, the Postal Service and DOD jointly implemented the Automated Military Postal System, which automates many military postal processes and provides detailed information on military post operations, transportation costs, and daily retail financial transactions. The system will reduce paperwork and labor costs, and improve timing and accuracy of air carrier payments.



FEDERAL RESERVE BOARD (FRB)

NS/EP TELECOMMUNICATIONS MISSION

The Federal Reserve Board's (FRB) NS/EP responsibilities relate to the "maintenance of the economic posture" and, in particular, the "maintenance of national monetary, credit, and financial systems." The FRB does not have telecommunications assets listed as NCS primary assets. Federal Reserve Banks, not the FRB, own or lease the Federal Reserve System's significant telecommunications assets.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Assistant Director of the IT program in the Board's Division of the Reserve Bank Operations and Payment Systems has responsibility for oversight of the Federal Reserve Banks' telecommunications services and serves as a liaison member on the NS/EPC.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The FRB supports NCS initiatives designed to provide essential telecommunications services needed to maintain the Nation's financial

telecommunications infrastructure and payment systems. The FRB continues to sponsor TSP assignments for essential telecommunications services supporting large-value payment systems, Federal Reserve open market and foreign operations, and the automated auction processing system for Treasury securities. The FRB sponsors the GETS for essential Federal Reserve Bank services and is currently participating in the interim WPS program.

SIGNIFICANT ACCOMPLISHMENTS

- The FRB focused its NS/EP activities on its sponsorship role in assigning TSP status, primarily at restoration level four, to essential telecommunications services under criteria it adopted in 1993. Following September 11, 2001, the FRB sponsored the priority provisioning of 108 circuits through the end of 2001. By the end of FY 2002, the FRB will have sponsored over 1,400 active TSP assignments.
- The FRB continues to sponsor a TSP assignment for circuits used for Fedwire funds transfer and securities transfer services, including access circuits to the Fedwire network from depository institutions that engage in large-dollar Fedwire transactions.
- The FRB continues to sponsor a TSP assignment for circuits used by other payment systems (e.g., the Society for Worldwide Interbank Financial Telecommunications and the Clearing House Interbank Payments System) that meet FRB's eligibility criteria.
- The FRB has implemented GETS across the Federal Reserve System to support communications within the Federal Reserve System and with depository institutions in the event of a disaster or communications disruption.



FEDERAL COMMUNICATIONS COMMISSION (FCC)

NS/EP TELECOMMUNICATIONS MISSION

The FCC NS/EP responsibilities include:

- Evaluating and strengthening measures for protecting U.S. telecommunications, broadcast, and other communications infrastructure and facilities
- Ensuring rapid restoration of U.S. telecommunications, broadcast, and other communications infrastructure and facilities after disruption by a terrorist attack or natural disaster
- Ensuring public safety, public health, and other emergency and defense personnel have effective communications services available in the immediate aftermath of any terrorist attack or natural disaster within the U.S.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Much of what the FCC does either directly or indirectly affects the NS/EP telecommunications activities of other Government departments and agencies. In the wake of the September 11 attacks, the FCC created the HLS Policy Council (HSPC) to further the Agency's NS/EP telecommunications mission. The HSPC has worked with other Government entities and with industry on HLS matters and coordinated Commission actions to improve HLS. Some of the most relevant of these actions are described below.

- **Rechartering the Network Reliability and Interoperability Council (NRIC):** The FCC rechartered the NRIC, a Federal Advisory Committee, to emphasize

the threats to network services and infrastructure caused by terrorist attacks and natural disasters. NRIC VI will develop best practices to aid in preparation for such threats and hasten restoration of network services in their aftermath. The composition of NRIC VI now includes representatives from a broader cross-section of the industry, including cable, wireless, satellite, and traditional wireline carriers.

- **Chartering the Media Security and Reliability Council:** The FCC chartered a "media counterpart" to NRIC, the Media Security and Reliability Council (MSRC). This consortium of broadcast, cable, and satellite companies first met in May 2002 and has goals similar to NRIC's.
- **Enhancing Public Safety Communications:** The FCC continued to work vigorously to improve public safety communications and interoperability in particular. For example, in FY 2002 the FCC adopted a joint Report and Order (R&O) that designates the 4940-4990 Megahertz (MHz) band for use in support of public safety; launched proceedings on solving public safety interference issues in the 800 MHz band and addressing future public safety issues in the 700 MHz band; adopted an R&O addressing the migration path to 6.25 Kilohertz technology by public safety licensees using the 700 MHz general use channels; and submitted a report to Congress on alternative frequencies for use by public safety systems and a report on critical infrastructure.
- **Implementing WPS:** The FCC granted a waiver permitting the initial implementation of WPAS,

which will alleviate the commercial wireless network congestion that NS/EP personnel experienced on September 11, 2001.

- **Implementing E911:** The FCC adopted Orders that grant waivers to six major national wireless carriers from certain initial Phase II E911 deadlines, while adopting revised, specific, and enforceable Phase II deployment schedules. It also announced further details of the technical inquiry to develop information on issues affecting the deployment of E911 systems for wireless callers.
- **Implementing Ultrawideband:** The FCC adopted an R&O establishing technical standards and operating restrictions for different types of ultrawideband (UWB) equipment, including rules permitting outdoor use of UWB devices in ground penetrating radars and other imaging systems to assist in emergency response and hostage rescue situations.
- **Furthering Communications Assistance to Law Enforcement Act Implementation:** The FCC adopted an Order on Remand finding that certain electronic surveillance capabilities mandated in the Communications Assistance to Law Enforcement Act proceeding must be provided by wireline, cellular, and broadband personal communications services carriers.



FEDERAL COMMUNICATIONS COMMISSION

(FCC) *continued*

SIGNIFICANT ACCOMPLISHMENTS

- Rechartered NRIC to emphasize threats to telecommunications network services and infrastructure.
- Chartered the MSRC to focus on threats to broadcast and cable media.
- Adopted an Order designating spectrum for use in support of public safety.
- Granted waiver permitting the initial implementation of WPAS.

A

ACRONYMS



A

NCS RELATED ACRONYMS

3

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2

A

ACE	Advanced Computing Environment
ACES	Access Certificates for Electronic Services
ACN	Alerting and Coordination Network
ACR	Alternate Carrier Routing
ADS	Air Defense Sectors
AEWS	Attack Early Warning System
AGCS	AG Communications Systems
AIN	Advanced Intelligent Network
ALE	Automatic Link Establishment
ANSI	American National Standards Institute
ARTCCs	Air Route Traffic Control Centers
ASD	Assistant Secretary of Defense
ASRs	Airport Surveillance Radars

B

BDT	Backup Dial Tone
-----	------------------

C

C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computer Systems
CAC	Common Access Cards
CCP	Classified Connectivity Program
CCPC	Civil Communications Planning Committee
CEO	Chief Executive Officer
CEPTAC	Civil Emergency Preparedness Telecommunications Advisory Committee
CERT	Computer Emergency Response Team
CHIPS	Clearing House Interbank Payments System
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPB	Critical Infrastructure Protection Board
CJCS	Chairman of the Joint Chiefs of Staff
CMS	Centers for Medicare and Medicaid Services

C (CONTINUED)

CMX-2002	NATO Crisis Management Exercise
----------	---------------------------------

CONR	Continental U.S. NORAD Region
------	-------------------------------

CONUS	Continental U.S.
-------	------------------

COOP	Continuity of Operations
------	--------------------------

COR	Council of Representatives
-----	----------------------------

COTP	Captains of the Port
------	----------------------

CTIA	Cellular Telecommunications and Internet Association
------	--

CWIN	Cyber Warning Information Network
------	-----------------------------------

CY	Calendar Year
----	---------------

D

DEA	Drug Enforcement Administration
-----	---------------------------------

DFOs	Disaster Field Offices
------	------------------------

DHS	Department of Homeland Security
-----	---------------------------------

DHHS	Department of Health and Human Services
------	---

DISA	Defense Information Systems Agency
------	------------------------------------

DISA-LAN	Defense Information Systems Agency Local Area Network
----------	---

DISN	Defense Information Systems Network
------	-------------------------------------

DITCO	Defense Information Technology Contracting Office
-------	---

DMAT	Disaster Medical Assistance Teams
------	-----------------------------------

DMS	Defense Message System
-----	------------------------

DOC	Department of Commerce
-----	------------------------

DOD	Department of Defense
-----	-----------------------

DOE	Department of Energy
-----	----------------------

DOENet	Department of Energy Corporate Network
--------	--

DOI	Department of the Interior
-----	----------------------------

DOJ	Department of Justice
-----	-----------------------

DOS	Department of State
-----	---------------------

DOT	Department of Transportation
-----	------------------------------

DS	Diplomatic Security
----	---------------------

DS/CMP/TSC	Diplomatic Security, Countermeasures Program Division, Technical Surveillance Countermeasure Branch
------------	---

DTS	Diplomatic Telecommunications Service
-----	---------------------------------------

E

EEOC	Equal Employment Opportunity Commission
------	---

eMLPP	enhanced Multi-Level Precedence and Preemption
-------	--

ENM	Enterprise Network Management
-----	-------------------------------

E.O.	Executive Order
------	-----------------

ERT	Emergency Response Training
-----	-----------------------------

ESFs	Emergency Support Functions
------	-----------------------------

ETS	Emergency Telecommunications Service
-----	--------------------------------------

ETSI	European Telecommunications Standards Institute
------	---

F

FAA	Federal Aviation Administration
-----	---------------------------------

FBI	Federal Bureau of Investigation
-----	---------------------------------

FCC	Federal Communications Commission
-----	-----------------------------------

FedCIRC	Federal Computer Incident Response Center
---------	---

FEMA	Federal Emergency Management Agency
------	-------------------------------------

FOC	Full Operating Capability
-----	---------------------------

FOIA	Freedom of Information Act
------	----------------------------

FRB	Federal Reserve Board
-----	-----------------------

FRP	Federal Response Plan
-----	-----------------------

FTR	Federal Telecommunications Recommendations
-----	--

FTS	Federal Technology Service
-----	----------------------------

FTS2000	Federal Telecommunications System 2000
---------	--

FTS 2001	Federal Telecommunications System 2001
----------	--

FTSC	Federal Telecommunications Standards Committee
------	--

FWUF	Federal Wireless Users Forum
------	------------------------------

FY	Fiscal Year
----	-------------

G

GCC	Group Communications Center
-----	-----------------------------

GETS	Government Emergency Telecommunications Service
------	---

G (CONTINUED)

GEWIS	Global Early Warning Information System
GIG	Global Information Grid
GISRA	Government Information Security Reform Act
GN	Ground Network
GPRA	Government Performance and Results Act
GSA	General Services Administration
GSC-IS	Government Smart Card - Interoperability Standard
GSM	Global System for Mobile

H

HF	High Frequency
HLS	Homeland Security
HPC	High Probability of Completion
HSPC	Homeland Security Policy Council

I

I&C	Information and Communications
IA	Information Assurance
IAM	Initial Address Message
IARS	Internet Anomaly Reporting System
IC	Integration Contractor
IEPS	International Emergency Preference Scheme
IES	Industry Executive Subcommittee
IETF	Internet Engineering Task Force
IG	Inspector General
IMA	Individual Mobilization Augmentee Program
INEEL	Idaho National Engineering and Environmental Laboratory
INFOSEC	Information Security
INMARSAT	International Maritime Satellite Organization
INS	Immigration and Naturalization Service
IOC	Immediate Operating Capability

IOSS	Interagency Operations Security Support Staff
IP	Internet Protocol
IPP	Internet Printing Protocol
IR	Industry Requirements
IRAC	Interdepartment Radio Advisory Committee
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
ISPG	Information Security Policy Group
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union's Telecom Standardization Sector
IXC	Interexchange Carrier

J

J6	Director for Command, Control, Communications, and Computer Systems Joint Staff
JCN	Justice Consolidated Network
JCS	Joint Chiefs of Staff
JS	Joint Staff

K

Kbps	Kilobits per second
KHz	Kilohertz
KMI	Key Management Infrastructure

L

LAN	Local Exchange Network
LEC	Local Exchange Carrier
LMBATF	"Last Mile" Bandwidth Availability Task
LMR	Land Mobile Radio
LNP	Local Number Portability
LRTF	Legislative and Regulatory Task Force

M

MAA	Metropolitan Area Acquisition Crossover Program
Mbps	Megabits per second

M

MHz	Megahertz
MSRC	Media Security and Reliability Council
MSS	Managed Security Services
MTSP	Multi-Tiered Security Profiles

N

NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center for Telecommunications
NCS RM	NCS Regional Manager
NCS	National Communications System
NDAC	Network Design and Analysis Capability
NDMS	National Disaster Medical System
NDO	NSIRC Desk Officer
NDRSMP	National Distress and Response System Modernization Project
NGN	Next Generation Network
NGS	Next Generation Strategy
NIAP	National Information Assurance Partnership
NIIF	Network Interconnection Interoperability Forum
NIPC	National Infrastructure Protection Center
NISN	NASA Integrated Services Network
NIST	National Institute of Standards and Technology
NORAD	North American Aerospace Defense Command
NPTF	National Plan Task Force
NRC	Nuclear Regulatory Commission
NRIC	Network Reliability and Interoperability Council
NSTISSP-11	National 1A Acquisition Policy
NS/EP	National Security and Emergency Preparedness
NS/EPC	Committee for National Security and Emergency Preparedness Communications

NSA	National Security Agency
NSC	National Security Council
NSIE	Network Security Information Exchange
NSIRC	National Security Incident Response Center
NSTAC	President's National Security Telecommunications Advisory Committee
NSVATF	Network Security Vulnerability Assessments Task Force
NTA	National Telecommunications Alliance
NTIA	National Telecommunications and Information Administration

O

OA	Operational Analysis
OC	Oversight Committee
OCA	Operational Certificate Authority
OEP	Office of Emergency Preparedness
OHS	Office of Homeland Security
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
OPSEC	Operations Security
OSD	Office of Security of Defense
OSM	Office of Spectrum Management
OTAR	Over-the-Air-Rekey

P

PAS	Priority Access Service
PBS	Public Buildings Service
PBX	Private Branch Exchange
PKI	Public Key Infrastructure
PMO	Program Management Office
PN	Public Network
POTS	Plain Old Telephone Service
PPBS	Planning, Programming, and Budgeting System
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
PT&E	Planning, Training, and Exercise

P (CONTINUED)

PTS	Priority Telecommunications System
-----	------------------------------------

R

R&D	Research & Development
R&O	Report and Order
RECP	Regional Emergency Communications Planner
RETCOs	Regional Emergency Transportation Coordinators
RFC	Request For Comments
RSPA	Research and Special Programs Administration

S

SAFECOM	Wireless Public SAFETY Interoperable COMMUNICATIONS Program
SHARES-HF	SHARED RESOURCES High Frequency Program
SIPRNET	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOCCs	Sector Operations Control Centers
SRWG	Security Requirements Working Group
SS7	Signaling System 7
SSU	Standing Subcommittee on Upgrades
STE	Secure Terminal Equipment
SXXI	Spectrum XXI
STU-III	Secure Telephone Unit-Third Generation

T

TAL	Test and Analysis Lab
TCS	Treasury Communications System
TIA	Telecommunications Industry Association

TIOC	Transportation Information Operations Center
TREAS	Department of the Treasury
TSCM	Technical Surveillance Countermeasures Mitigation
TSP	Telecommunications Service Priority
TSS	Telecommunications Services Staff

U

UHF	Ultra-High Frequency
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture
USMS	U.S. Marshals Service
USPS	U.S. Postal Service
UWB	Ultrawideband

V

VA	Department of Veterans Affairs
VANTS	VA Nationwide Teleconferencing System
VHF	Very-High Frequency
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

W

WAN	Wide Area Network
WDA	Watch Desk Analysis
WLAN	Wireless Local Area Network
WMD	Weapons of Mass Destruction
WPAS	Wireless Priority Access Service
WPS	Wireless Priority Service

**National Communications System
(NCS)**

**701 South Courthouse Road
Arlington, VA 22204-2198**

<http://www.ncs.gov>

